NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ANALYSIS OF JORDAN'S PROPOSED EMERGENCY COMMUNICATION INTEROPERABILITY PLAN (JECIP) FOR DISASTER RESPONSE

by

Mohamad H. Alzaghal

December 2008

Thesis Co-Advisors: Rex Buddenberg
Brian Steckler

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Analysis of Jordan's Proposed Emergency Communication Interoperability Plan (JECIP) for Disaster Response.			**5. FUNDING NUMBERS**
6. AUTHOR(S) Mohamad H. Alzaghal			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S.. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Recently, the world has been affected by man-made and natural disasters of a level not shown before which depicts the importance of communication for an efficient and rapid response of First Responder Community (FRC) members in the field.

The resilience of communication infrastructure is vital for the well being of any country. It is essential to build a robust and interoperable Information and Communication Technology (ICT) infrastructure before the disaster, which will facilitate patch/restore/reconstruct it when and after the disaster hits.

Overviews for most ICT standards currently available are introduced. This background is needed for any emergency communication interoperability plan.

Training is very important so that staffs will be ready when needed to implement the emergency plans. Exercises such as Strong Angel III (SAIII) are always the best approach to explore different ICT systems and these systems resilience in the case of disaster in the context of power, range, and interoperability.

The Hashemite Kingdom of Jordan (Jordan) may benefit from studying the U.S's experience in emergency communications and may consider modifying its communications interoperability plans and improve its infrastructure to enhance readiness for disasters. The author explored Jordan's current emergency communications interoperability plans, policies, Emergency Operation Plans (EOPs) and compares Jordan's HA/DR communications readiness level versus that of the U.S.

Based on the technological aspects of emergency communications, Jordan's communications environment, the requirements analysis of emergency communications plan, and lessons learned from the U.S. experience, a proposed Jordan Emergency Communications Interoperability Plan (JECIP) is introduced in this thesis.

14. SUBJECT TERMS Hastily Formed Networks (HFN), Stability & Reconstruction (S&R), Humanitarian Assistance/Disaster Relief (HA/DR), Jordan's Emergency Communications Interoperability Plan (JECIP), Emergency Operation Plans (EOPs), First Responders Community (FRC), Information and Communications Technology (ICT).	**15. NUMBER OF PAGES** 127
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ANALYSIS OF THE PROPOSED JORDAN'S EMERGENCY COMMUNICATION INTEROPERABILITY PLAN (JECIP) FOR DISASTER RESPONSE

Mohamad H. Alzaghal
Lieutenant Colonel, Jordan's Armed Force (JAF)
B.S., Mu'tah University, 1988
M.S. in Electrical Engineering, NPS, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRONIC WARFARE SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2008

Author: Mohamad H. Alzaghal

Approved by: Rex Buddenberg
Thesis Advisor

Brian Steckler
Co-Advisor

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Recently, the world has been affected by man-made and natural disasters of a level not shown before which depicts the importance of communication for an efficient and rapid response of First Responder Community (FRC) members in the field.

The resilience of communication infrastructure is vital for the well being of any country. It is essential to build a robust and interoperable Information and Communication Technology (ICT) infrastructure before the disaster, which will facilitate patch/restore/reconstruct it when and after the disaster hits.

Overviews for most ICT standards currently available are introduced. This background is needed for any emergency communication interoperability plan.

Training is very important so that staffs will be ready when needed to implement the emergency plans. Exercises such as Strong Angel III (SAIII) are always the best approach to explore different ICT systems and these systems resilience in the case of disaster in the context of power, range, and interoperability.

The Hashemite Kingdom of Jordan (Jordan) may benefit from studying the U.S's experience in emergency communications and may consider modifying its communications interoperability plans and improve its infrastructure to enhance readiness for disasters. The author explored Jordan's current emergency communications interoperability plans, policies, Emergency Operation Plans (EOPs) and compared Jordan's HA/DR communications readiness level versus that of the U.S.

Based on the technological aspects of emergency communications, Jordan's communications environment, the requirements analysis of emergency communications plan, and lessons learned from the U.S. experience, a proposed Jordan Emergency Communications Interoperability Plan (JECIP) is introduced in this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Professor Rex Buddenberg and Professor Brian Steckler for their help and guidance throughout this thesis work.

Also, I would like to thank my wife Nahla Alawadat and family for their understanding and constant support.

Last but not least, I wish to dedicate this work to the soul of my late father, Hisham Alzaghal, for all of his efforts throughout his life for his family.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Recently, the world has been affected by man-made and natural disasters of a level not shown before which depicts the importance of communication for an efficient and rapid response of First Responder Community (FRC) members in the field.

The resilience of communication infrastructure is vital for the well-being of any country. It is essential to build a robust and interoperable Information and Communication Technology (ICT) infrastructure before the disaster, which will facilitate patch, restore, and reconstruct it when and after the disaster hits.

Overviews for most ICT standards currently available are introduced. This background is needed to furnish for emergency communication interoperability plan.

Training is very important so that FRC members will be ready when implementing the emergency communications plans. Exercises such as Strong Angel III (SAIII) are normally an excellent approach to explore different ICT systems and its resilience in case of disaster in the context of power, range, and interoperability.

Jordan may benefit from studying the U.S.'s experience in emergency communications and may consider modifying its communications interoperability plans and improve its infrastructure to enhance readiness for disasters. The author explored Jordan's current emergency communications interoperability plans, policies, Emergency Operation Plans (EOPs) and compares Jordan's HA/DR communications readiness level versus that of the U.S.

Based on the technological aspects of emergency communications, Jordan's communications environment, the requirements analysis of emergency communications plan, and lessons learned from the U.S. experience, a proposal for Jordan's Emergency Communications Interoperability Plan (JECIP) is introduced in this thesis.

The Humanitarian Assistance/Disaster Relief (HA/DR) environment, peacekeeping, or Stability & Reconstruction (S&R) activities are aspects of the interoperability plan as Jordan is also playing a big role in UN peacekeeping missions.

The current emergency communications interoperability plan needs to be revised to account for new methods and techniques of response to various emergencies both

internally within Jordan and in terms of potential interoperability in a multi-national peacekeeping or HA/DR response such as the Pakistan earthquake of February 2006 or the Southeast Asia tsunami of December 2004.

A. BACKGROUND

The Southeast Asian tsunami, Hurricane Katrina, and the 2006 Pakistan earthquake have emphasized the need for efficient communications and triggered improvements in this field. ICT systems are vital for response time reduction and to increase chances for an efficient usage of resources.

Another domain for emergency communications interoperability planning is the United Nation (UN) peacekeeping missions. Jordan along with other countries is contributing to these missions all over the world and we all have to work together in the same HA/DR environment. The peacekeeping forces are deployed most of the time in areas with no ICT infrastructure and need a plan which articulates policies, capabilities, and technologies to build an interoperable ICT network that would help the troops conducting their humanitarian role in harmony with other agencies and local government.

B. OBJECTIVES

The objective of this thesis is to study current infrastructure capabilities in Jordan to facilitate building an interoperable ICT infrastructure which is resilient to disasters. ICT systems that are interoperable with other nations in a possible multi-national disaster response, especially in peacekeeping missions, are vital for the purpose of more efficiency and reliability in responding to an emergency. Jordan may benefit from the lessons learned and plans revised after Katrina in U.S. and could use these lessons to create a better emergency communications interoperability plan.

C. RESEARCH QUESTIONS

The research questions to be addressed in this thesis are outlined into three categories:

1. Survey

a. What are the concepts and terminologies used in emergency communications for disaster response?
b. What are the new technologies that may be used to enhance communication infrastructure resilience and patch in case of emergency?
c. What is Jordan's ICT environment?

2. Analysis

a. What are the requirements for a better emergency communications interoperability plan in Jordan?
b. How can Jordan use the U.S. expertise in the domain of emergency communications interoperability?
c. What should Jordan do to improve its preparedness in the domain of emergency communications interoperability and what are the guidelines to build a viable emergency communications interoperability plan for Jordan?

3. Synthesis

a. What is the emergency communications interoperability plan for an interoperable infrastructure in Jordan?

D. THESIS ORGANIZATION

Again, this thesis is organized into the three categories mentioned above:

1. Survey

This category is divided into four chapters: Chapter II discusses disaster response Preparedness: Training & Exercises. Lessons learned from U.S. experience are elaborated in Chapter III. Chapter IV surveys emergency communications interoperability plan requirements. Communication technologies overview is elaborated in Chapter V.

2. Analysis

This category is comprised of Chapter VI; titled as Jordan's Information and Communications Technology (ICT) Environment.

3. Synthesis

This category is divided into two chapters: Jordan’s Emergency Communications Interoperability Plan (JCIP) is proposed in Chapter VII. Conclusions and future works are presented in Chapter VIII.

II. DISASTER RESPONSE PREPAREDNESS: TRAINING & EXERCISES

Disasters usually happen by surprise. For this reason, the First Responders Community (FRC) should have or obtain the proper training and education in their specialty. It is important that all personnel from all agencies concerned with disaster response learn the same language and terminologies used in the emergency management community.

This may be called “procedural interoperability” which is different from “communications interoperability.” FRC members are trained on Incident Command System (ICS) for the purpose of better procedural interoperability among them as they may be responding to a disaster or other event from different agencies and sometimes from different countries [4].

Scholars and researchers often study disasters that have already happened to extract the lessons to be learned and try to identify the flaws to be avoided in the future.

In this Chapter, disaster response training and exercises are elaborated as part of the study process of this thesis. Definitions and terms used in these events and in this learning process are to be embedded in this thesis — terms such as Hastily Formed Network (HFN), HA/DR, Stability & Reconstruction (S&R), etc., so that the reader can follow the information presented.

Training is very important so that staffs will be ready when needed to implement the emergency plans. Exercises are often the best approach to get the best training in the emergency domain as theory by itself without proper testing will not be enough.

In this thesis, communications training for better interoperability is focused on. There are three communications equipment training categories: maintenance, operations, and the procurement process. User requirements for the communication systems to be acquired are the responsibility of the agency; which need a knowledgeable staff in this regard. System requirements are the task for the vendors of these systems.

A. STRONG ANGEL III (SAIII) [3]

As part of this thesis study, the author participated in the SAIII exercise as an observer. SAIII was held at San Diego, California, USA from 21 to 26 of August 2006. Multiple locations were used to simulate a widespread epidemic in the city accompanied by a cyber attack on the communications infrastructure and information systems.

This exercise was a very rich experience as it was a gathering of numerous elite companies, government agencies, and Non-Government Organizations (NGOs). The Strong Angel III exercise was a series of experiments implemented with an assumption of response to a disaster. Participants were volunteers from both public and private sectors. The experiments and demonstrations enhanced the integration of technologies and techniques for information flow and cooperation between different companies, government, NGOs, and militaries to fulfill the goal of fast and efficient humanitarian relief for victims of natural disasters and wars.

The Strong Angel idea was started after the Kosovo refugee migration. The problems facing the responders in the field were put together and addressed. Participants worked on solutions at Strong Angel I (SAI) which took place in Hawaii, USA in June of 2000. SAI simulated a refugee camp with a distributed medical intelligence communications infrastructure. Strong Angel II (SAII) was held in Hawaii, USA in the summer of 2004.

Figure 1. A photo from SAIII opening (From: [3]).

These locations were connected using different technologies to test reliability and resilience of ICT systems throughout the course of implementation of the different tasks of SAIII. SAIII tried to match people in need of solutions to problems (experienced when working with disasters such as the Tsunami) with people who had solutions to those problems.

Solutions were not necessarily technology-based. Some of the problems could be solved using social networks or building trust at a human to human level between parties working on the tasks. Some of the companies were exploring a method to integrate their solutions with other companies' solutions which would make these solutions more robust and efficient.

This SAIII exercise tried to generate ideas and techniques that would overcome boundary problems, such as public/private sector partnership, local/non-local authorities, national/international domain members, and civil/military relationships. Other common problems that were dealt with included networks, geography, language, and culture.

While Information and Communications Technology (ICT) systems were a key issue addressed during SAIII, there were approximately fifty technical tasks addressed by

SAIII's leadership team. Loss of communications during an emergency response is devastating to the whole mission. Technologies and techniques are needed to address this important issue.

Different solutions and platforms were tested and challenged. Communications networks, including ad-hoc mesh networks, SMS text messaging, and wireless systems technologies were employed. Interoperability, integration, mobility, power supplies, imaging, and mapping were the main technological challenges focused on during the SAIII exercise.

The core of the exercise which is relevant to our research was the disruption in the normal communications. Regardless of the specific applications (such as chat and e-mail) used by the First Responders Community (FRC) members; the basis is ICT infrastructure restoration. Participants had to patch the communications infrastructure up utilizing technologies offered by vendors.

B. THE CEBROWSKI INSTITUTE FOR INNOVATION AND INFORMATION SUPERIORITY [15]

Located at the Naval Postgraduate School (NPS), Monterey, CA, USA; the Cebrowski Institute for Innovation and Information Superiority has organized a weekly gathering throughout Fiscal Year 2006 to discuss the research and projects surrounding the concept of Hastily Formed Networks (HFN).

This series of group discussions hosted speakers from different disciplines and agencies related to the domain of disaster management. Some of these concepts are explained here:

1. Hastily Formed Networks (HFN)

Networks typically mature slowly and they can be enhanced through continuous observation during their lifetime. HFN is a network that is formed and configured rapidly in response to emergency situations with limited life span. HFNs must be prepared and designed before they are needed. Despite their limited life span, it is possible to identify best practices in how they can be effectively prepared, staffed, and executed [15].

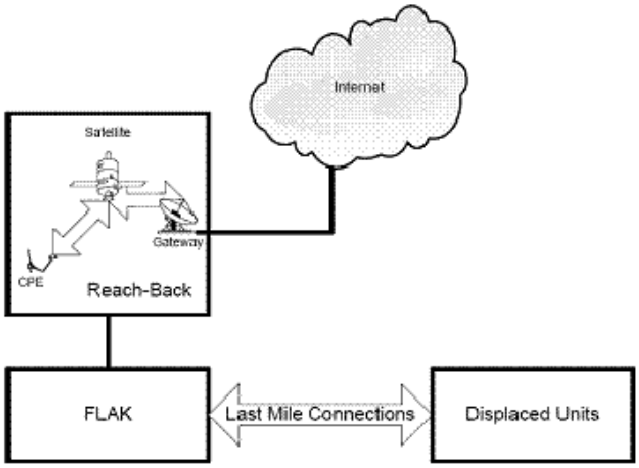

Figure 2. Three Basic HFN Components: Reach-Back, Last-Mile, and Fly Away Kit (FLAK) (From: [16]).

HFN networks maintenance philosophy, personnel training, procurement strategy, and security should be clear to all agencies so they will not improvise and will not work in disarray in case of disaster.

2. Humanitarian Assistance/Disaster Relief (HA/DR)

HA/DR is a concept which can be measured to evaluate the level of services offered by the First Responders Community (FRC) to victims in the field based on two dimensions: time & location. High level of HA/DR means less time elapsed for help to arrive at the location of a disaster.

HA/DR includes all actions taken in terms of humanitarian aid assistance, evaluating medical needs, underlying economic concerns, and works together to help the people affected by the disaster.

3. Stability & Reconstruction (S&R)

The term S&R includes capacity enhancement, training, and infrastructure reconstruction programs such as restoring electricity and normal Internet infrastructure in post-disaster environment (without the disaster patches) and to train maintenance staff for it.

4. Stability, Security, Transition & Reconstruction (SSTR)

The SSTR concept has more roles added to the S&R definition in terms of enhancing local and regional security capacity through collaborative efforts. Transitions deal with critical time frames in the case of cease fire negotiation between parties, or the time frames after a natural disaster and before the active reconstruction plans are implemented.

5. Complex Humanitarian Emergency (CHE)

CHEs are man-made disasters (such as civil or other wars) which cause mortality and destruction more than most natural and technological disasters. It is important for the international agencies in this case to understand the political and social situation in the disaster region. Health care is one of the key issues in this kind of emergency.

6. Complex Humanitarian Disaster (CHD)

CHDs are natural event caused disasters, which can be unpredictable in terms of time and size. The key issue in this kind of disaster is time, as assistance can take a lot of time to be sent to remote locations.

7. Social Networks

While technology is an important aspect of the emergency response in terms of providing people in the field with communication and data networks with high availability and robust continuous service, human resources are also extremely important and vital for the success of the mission. Building social networks will make use of these systems and facilitate the implementation of the objectives on the ground.

8. Critical infrastructures and Key Resources (CI/KR) Protection for Disaster Reduction

The definition of Critical Infrastructures and Key Resources (CI/KR) “is organizations and facilities of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences” [22].

The outcome of hazard and vulnerability analysis for the Critical Infrastructure (CI) will be a pyramid, which depicts the effect of the asset on the life of population, especially in case of disasters. Each country or enterprise should categorize their assets and rank them according to the pyramid shown in Figure 3. Note that communication infrastructure is starting to climb up to the top.

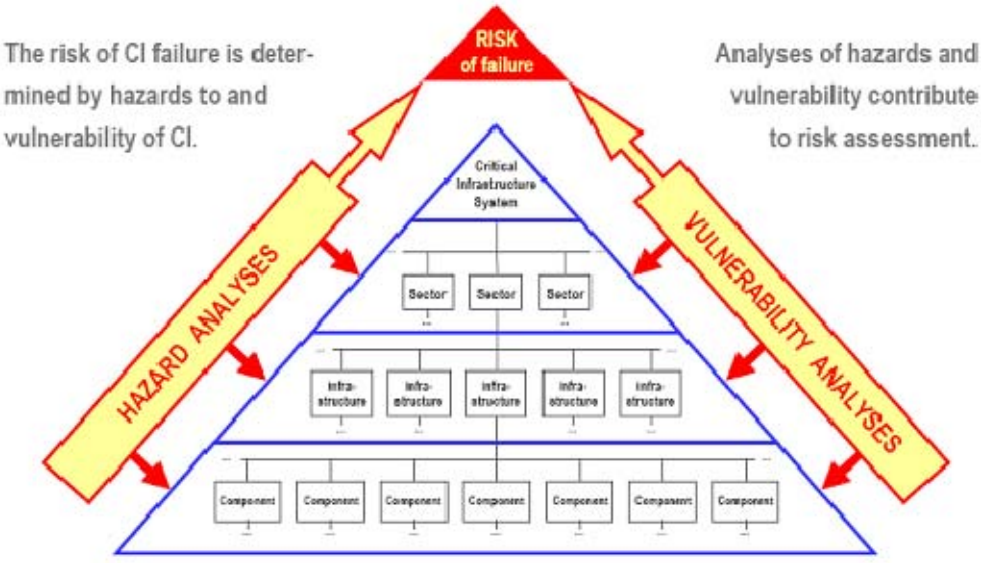

Figure 3. Critical Infrastructure Risk of Failure (After: [22]).

9. The Disaster Risk Management Cycle (DRMC)

The Disaster Risk Management Cycle (DRMC) clarifies how the stages: Pre-Disaster, Response, and Post-Disaster correlate with Risk Assessment, Mitigation, Preparedness, Warning/Evacuation, and Assessing Damage. The threshold point in this cycle is the Warning/Evacuation point. If this point is accurately predicted, a lot of people will be saved and immediate assistance will be provided to them. Figure 4 depicts the disaster risk management cycle [25].

Figure 4. The Disaster Risk Management Cycle (From: [25]).

C. FIRST REGIONAL MEDICAL CONFERENCE ON DISASTER MANAGEMENT

Organized by the Jordanian Royal Medical Services (JRMS) of Jordan's Armed Forces (JAF), the First Regional Medical Conference on Disaster Management was held in Amman-Jordan from November 1-3, 2007. The author participated by submitting a paper titled "Analysis of Jordan's Emergency Communication Interoperability Plan (JECIP) for Disaster Response."

Although the main theme of the conference was medical aspects of disaster management, several papers discussed issues such as: "Using Computer Modeling and Simulation as a Foundation of Disaster Preparedness," "National Strategy for Emergency Preparedness in Jordan," and other subjects.

Participants from several countries such as the U.S., Turkey, UAE, and Palestine exchanged their experiences and knowledge. Part of the conference was an exercise conducted by the Jordanian Royal Medical Services (JRMS) along with the Corps of Engineering of JAF and other agencies. The scenario of the exercise was comprised of a chemical attack and the evacuation of casualties out of the area as well as apparent contamination to hospitals [42].

The conference emphasized the fact that telemedicine and other related applications will not work without a robust and interoperable communications infrastructure.

D. SUMMARY

In this chapter, terms and concepts in the context of First Responders Community (FRC) were elaborated on so that the reader will have the minimum background for the following discussions of disaster recovery and the communications field.

THIS PAGE INTENTIONALLY LEFT BLANK

III. LESSONS LEARNED FROM U.S. EXPERIENCE IN EMERGENCY COMMUNICATIONS INTEROPERABILITY

Jordan and the U.S. are different in size, economy, and government organization; but many of aspects of disaster management are still valid for both countries.

The concepts and objectives in the two countries' emergency interoperability communications plans are almost identical. The differences between them are due to the different political systems which will result in a change of the chain of command and responsibilities. Another reason for the difference is the technical and funding levels of both countries.

In this chapter, the U.S. experience in emergency communications interoperability is elaborated on. Other concepts such as modularization model, interoperability types used by agencies when they cannot talk to each other, and the procurement process for interoperable communications equipment are also presented.

A. INFORMATION SYSTEM MODULARITY MODEL [1]

The First Responders Community (FRC) relies on voice radio in communicating with each other in the field while ignoring issues such as trunking multiple conversations. Packet-Switching (becoming the dominant over Circuit-Switching (CS)) as voice is considered as an application of Voice over Internet Protocol (VoIP).

To enhance interoperability, a common modularity model or architecture between multiple agencies is needed. The standards are only the means to define the interfaces.

The core requirement for interoperability of the communications network is that all the segments be routable networks such as WiMAX, WiFi, and all of the cabled Internet technologies.

Radio-Wide Area Networks (Radio-WANs) requires specific characteristics to be used in emergency situations. Outside characteristics: Each segment should be a routable network. Internal characteristics: Stable Media Access Control (MAC), ability to Multicast, infrastructure protection security, and fault detection.

The objective of architecture is to prescribe a common modularization model for all information systems. The main goal achieved by this modularization is a decoupling of the end systems from the radio-WANs. A good modularized component should have the following interfaces:

1. LAN Interface

Routable interfaces; such as Ethernet interface; is the common LAN interface. Non-routable data links are not a plausible solution.

2. Messaging or Data Packaging Interface

E-mail user agents support digital signature and encryption (Public and Private Keys).

3. PKI Interface

In information systems, authenticity mechanism is of core importance. Confidentiality requires additional to authenticity.

4. QoS Interface

QoS is not necessary for end systems if the best effort delivery mechanisms of the Internet are adequate.

5. Management Interface

Simple Network Management Protocol (SNMP) interface is in the form of the required Management Information Base (MIB).

B. INTEROPERABILITY REFERENCE MODEL (IRM) [1]

Information and Communications Technology (ICT) systems interoperability needs standards to articulate the module boundaries after the modularization is performed. There are two backdrops of standards: the first is to use standards to dictate technology choices. The second is to use standards to avoid modularity.

Similar to the ISO Reference Model, the Interoperability Reference Model (IRM) is intended to perform the same function for interoperable information systems as the ISO Reference Model does for interoperable networks to organize the discussion. Table 1 depicts the model components.

The top three elements in the IRM are based on human factors while the bottom four layers are based on Command, Control, Communications, Computer, and Intelligence (C4I). The objective of IRM is to create an information system with a set of interchangeable parts that can be assembled and reassembled (this can be called a prescriptive architecture).

1	Doctrinal interoperability	A human factor that leads to coherency and uniformity of action.
2	Cognitive or shared situational awareness	Information systems are interoperable at this layer if decision makers in two different systems are seeing coherent pictures of the information presented.
3	Interoperable procedures	This is the domain long inhabited by Standard Operating Procedures (SOP) or Tactics, Techniques & Procedures (TT&P).
4	Shared processes	This is a software engineering concept. At its trivial level reusable code obviously enhances interoperability but that is a side effect of what is essentially an economy effort in code production.
5	Data Element interoperability	It is a clear requisite to information system interoperability.
6	Information system modularity	Refers to development of a complex product (or process) from smaller subsystems that can be designed independently.
7	Internetworkability	Communications interoperability can be defined by ability to Internetwork.

Table 1. A Proposal for an Interoperability Reference Model (IRM) (After: [1]).

1. Doctrinal Interoperability

Doctrinal interoperability is a human factor that leads to coherency and uniformity of action. When different decision makers are exposed to the same

information, they will make similar decisions. This model abstracts discussion to where it belongs and will not eliminate the doctrinal tensions of uniformity against creativity. This layer may be divided into tactical, operational and strategic sub-layers.

2. Cognitive Interoperability

Cognitive interoperability is based on shared situation awareness between decision makers; as if they see a coherent picture of the information presented, the information systems will be interoperable.

3. Interoperable Procedures

This layer is comprised of Standard Operating Procedures (SOP) or Tactics, Techniques & Procedures (TTP's). An example for this layer, multi-agency Command and Control, is enhanced by an Incident Command System (ICS) used by emergency service providers.

4. Shared Processes

A software engineering concept for code production, reusable code enhances interoperability especially for mobile and portable code. SOA or SaaS or ERP inhabits this layer (although they may overlap into others).

5. Data

Data element interoperability and coherent data dictionaries are essential for information system interoperability.

6. Modularity

Modularity refers to smaller subsystems that can be designed independently to develop a complex system. Poor modularization manifests itself in poor life cycle maintainability. Two steps are necessary for reusable components:

First: decoupling of end systems from the communications; which allows the change of one subsystem without the other. Second: modularity between end systems; which allows the usage of a Sense module from one information system to feed data to a Decision one in another.

7. Internetwork

Communications interoperability is based on Internetworkability between two systems.

C. U.S. EXPERIENCE IN INTEROPERABILITY ENHANCEMENT

In the U.S., the Office for Interoperability and Compatibility (OIC) of the Department of Homeland Security (DHS) initiated a national communications program (SAFECOM) to bring focus to interoperability issues. Communications interoperability is defined by the SAFECOM program as follows: "The ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when needed, and as authorized."[18]

1. The National Taskforce on Interoperability (NTFI).

Following the 9/11 incident in the U.S., the National Institute of Justice (NIJ), Office of Science and Technology organized the National Task Force on Interoperability (NTFI), a task force that has members from eighteen national associations that address the problem of communications interoperability.

NTFI conducted many studies on emergency communications interoperability and reported out five important reasons why the public safety agencies cannot talk to each others. They are as follows [18]:

a. Incompatible Equipment

Incompatible and aging communications equipment used by agencies and at the same time, neighboring agencies have migrated to higher frequency bands, digital channels, and trunked systems causes the lack of interoperability. Replacing the equipment with routable networks will solve this problem.

b. Limited and Fragmented Funding

Lack of funding will hinder the replacement of aging incompatible equipment, restricting human resources available, focusing on internal operational needs, limiting access to the frequency spectrum resources.

c. Limited and Fragmented Planning

Lack of planning will result different agencies competing for limited funds which will provide few resources for inter-agency planning efforts and that may compound the interoperability problem by demoting cooperation and joint operating plans that define communications needs.

d. Lack of Coordination and Cooperation

To promote coordination, certain steps may be taken: reduce isolated spending, increase sharing of management and control, and enhance infrastructure sharing such as towers and sometimes full systems.

e. Limited and Fragmented Radio Spectrum

ICT systems are technologically incompatible at a fundamental level if they are using different frequency bands. Agencies seeking to upgrade their systems are forced to move to a higher frequency bands to find available channels.

2. Reactive Inter-agency Interoperability Types

The SAFECOM program has identified five critical elements to solving inter-agency communications problems: Governance, Standard Operating Procedures (SOPs), training and exercises, frequency of use, and technology. There are five technological means of inter-agency communications: swapping radios, using gateways between independent systems, sharing channels, sharing proprietary systems, and sharing standard-based systems [18].

Interoperability types used by agencies when they cannot talk to each others may be defined by the public safety community in the following variants:

a. Swap radios (SR)

The dispatching or responsible agency for the Command, Control, and Communications (C3) in the field will swap radios when other FRC members arrive at the location of a disaster.

b. Talkaround (TKR)

When losing the ability to talk back to the dispatch center, FRC members may utilize the radio-to-radio functionality.

c. Mutual Aid Channel (MAC)

In case of agencies which operate on separate frequencies, these channels have set aside frequencies and pre-programmed them to utilize these channels in case of inter-agency communications during the event.

d. Gateway Console Patch (GCP)

The gateway console is designed to patch two or more radio systems to communicate in case of emergencies. There are many types of GCP such as: interface with other Radio Frequency (RF) links, 4-wire audio links, and Voice over Internet Protocol (VoIP) links.

e. Network Roaming (NR)

Network roaming is when the infrastructure topology is based on a single common air interface; which is able to accept multiple vendors' mobile equipment.

f. Standards Based Shared Networks (SBSN)

Standards may be used as a baseline for an evaluation tool for system levels of interoperability. An example for these standards is Project 25 (P25) published by the Telecommunication Industry Association (TIA) and is an industry standard for voice and data transmissions.

3. Communications Interoperability Project Management

When planning for communications interoperability, there are elements to be considered in that project: field operations radio users, field operations command staff, executive officers of fire; police; and medical agencies, dispatch management, technical support staff, emergency management officials, elected officials, media, and the public.

These projects are very difficult to manage because they are large, expensive, and multi-agency in nature, are built on a variety of complex technologies, require environmental/historical and cultural assessments of sites, and finally depend on frequency licenses. In the balance life or death may be on the line out of these services.

To build an interoperable communications infrastructure, four questions need to be answered regarding the plan project [18]:

a. What?

A needs analysis is the organized process of collecting information on what interoperable system needs.

b. Why?

ICT systems interoperability is achieved through a system of systems (technological and operational).

c. Who?

Agency executives and senior managers should build this foundation of agreement.

d. When?

Immediately, as nobody knows when a disaster strikes or when funding may go to a less important project.

There are steps to conduct interoperability needs analysis: determine user needs, develop operational requirements, and evaluate build-versus-buy options. To build a plausible interoperability project, a survey for existing radio sites is needed in the

following context: Safety and security of the site permits legitimate maintenance and may keep away unwanted visitors, so the question must be asked whether or not there is e a space for the antenna systems? Further, does the equipment rack have space for radios and combining equipment?

To find out if the power distribution units suit the needs for the site, the electrical Radio Frequency (RF) grounding should meet the industry standards, to make sure that the site has a suitable monitoring system for tower lights, power systems, and security controls.

Communication interoperability depends on evolving factors such as level of communications needs, developing technologies (especially wireless networks), and the public understanding of those concepts.

Communications technical requirements could be categorized and defined with one or more qualities, such as the following:

To plan for enhanced interoperability, key elements should be addressed. A concept of Interoperability Continuum gathers these elements for successful planning for a robust interoperability solution as depicted in Figure 5. Technology, training, equipment, Standard Operation Procedures (SOPs), and governance are some of these key issues. When procurement for new equipment should be proposed, this proposal will include plans for the training on that equipment so that it will be used efficiently [18]:

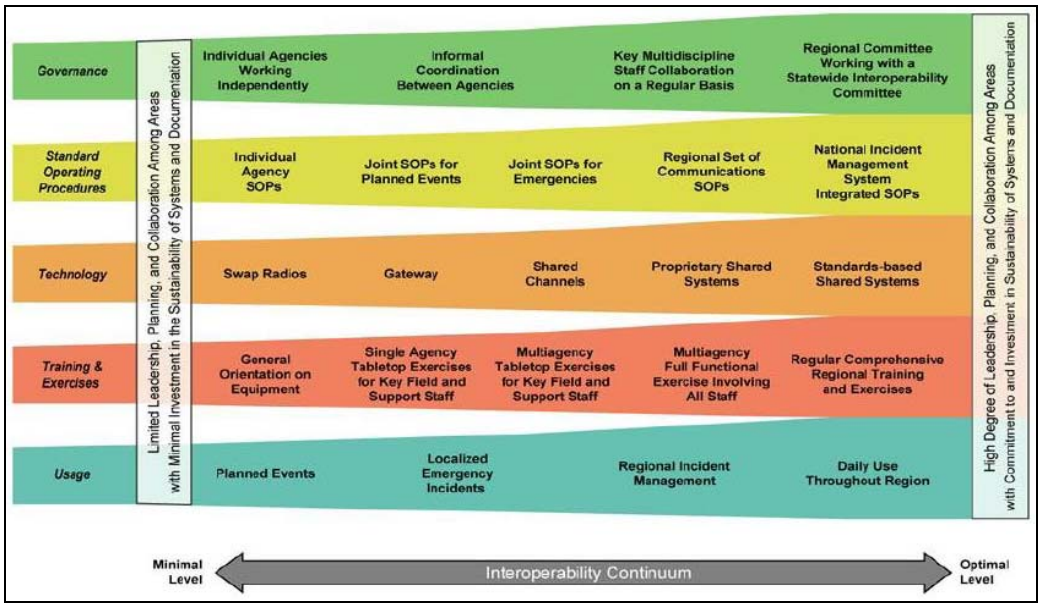

Figure 5. Interoperability Continuum (From: [18]).

D. PROCUREMENT PROCESS FOR INTEROPERABLE COMMUNICATIONS EQUIPMENT

For the equipment acquisition process, Jordan may benefit from the U.S. procurement cycle. U.S. federal government uses the Indefinite Delivery, Indefinite Quantity (IDIQ) contracts. This means that one vendor will be awarded a contract which will be open for other agencies to acquire equipment with the same terms and conditions.

In other words, Telecommunications Regulatory Commission (TRC) of Jordan, for example, is to award a contract to a vendor with a promise to buy a minimum amount off the contract to make it economical for that vendor. The contract is then opened to all agencies in Jordan so they will buy from the same source. IDIQ is a procurement process that brings interoperability through commonality [40].

To assure vendors eligibility, some sort of interoperability testing mechanism is needed. The U.S. Department of Defense (DoD) conducts this process through their Joint Interoperability Test Center (JITC) [43].

Interoperable communications between agencies during mutual aid events is the aim of this procurement process. Good modularization is mainly achieved through to isolating requirements into smaller independent units. The procurement process may be categorized as follows [40]:

1. Gathering Information

The first step is to gather information about the existing ICT infrastructure needs, available assets and resources, and end user requirements.

An inventory of all of existing ICT systems hardware and software and frequency licenses is necessary to procure new systems. The inventory should include as many of the following as possible: quantity, manufacturer, make, and model, year of installation/purchase, year last upgraded, frequency of use, purpose, location, owner, user, original cost, and estimated remaining useful life.

2. Capabilities Forecast

Capabilities analysis of the new system is to identify if there are new capabilities to be added to the existing system and who will use them.

Important capabilities to be required in the new system: backward compatibility with existing technology, compliance with operational; functional; and technical standards, ability to accommodate peak usage needs, and end-user support for equipment that includes handheld portable radios and vehicle-mounted mobile radios.

3. Cost Prediction

Price and value concepts are different from each other. The purchase price of the equipment or service alone is not sufficient to understand how much a system will cost over a 15-year period. Total Life Cycle Costs (TLCCs) is an important concept to take into consideration. TLCC is a way to measure how much the system will cost over its expected life.

Value is a better concept which includes: purchase price, quality, warranties, and cost of the following: maintenance, training, service, along with hidden costs such as response time, reliability, company stability, delivery time, and contract terms and conditions.

4. Joint Effort to Fund Communications Infrastructure

The government should encourage this type of joint procurement between agencies which will enhance interoperability and reduce prices due the economy of scale principle.

5. Identifying the Project's Benefits

It is important to justify the new ICT project by identifying its tangible benefits (decreased maintenance costs of old systems, improved coverage of service, and interoperability) and the intangible benefits (better morale, better customer service).

6. Gap Analysis

When the needs assessment is accomplished, a comprehensive gap analysis of the communications infrastructure should list what technologies may be able to meet the operational requirements of the agency. The next step is the draft of Request for Proposal (RFP).

7. Request for Quotation (RFQ) and/or a Request for Proposal (RFP)

Vendors respond to the RFQ with a bid or to the RFP with a proposal. RFP process should be started based on vendor neutral user requirements.

The RFP should include the description of the following: Problems, Environment, (e.g., existing equipment, operational procedures, agency standards, and constraints), project outcome, scope (i.e., user functionality, system response times, delivery schedule, service levels, and training).

8. Proposal Evaluations

An evaluation criterion should be defined before the reception of proposals. Proposals should be evaluated against that criterion to select the proposal that best meets the defined needs and requirements.

9. Vendor Selection

When a single vendor emerges from the evaluation criterion, contract negotiation is the next step. If more than one vendor succeeds, additional interviews are needed to select the best one.

10. System Delivery

The system should be delivered through a test plan. Factory Acceptance Test (FAT) and Field Acceptance Test (FIAT) are important to be conducted to make sure that the vendor's design of system requirements complies with the user requirements.

E. CONSTRAINTS FACED BY EMERGENCY COMMUNICATIONS [44]

The obstacles and problems facing communications in Jordan during disasters may be categorized into four types– institutional, regulatory, technical, and financial. There will be a strategy to deal with all of these constraints through the crafting of the emergency plan.

1. Institutional Constraints

A comprehensive disaster management format is needed especially in the context of immediate actions, long-term preparedness, and general disaster planning. Creating organizational structure for disaster management enables one to determine which agencies are more equipped to deal with emergencies. Better inter-agency coordination is also essential.

2. Regulatory Constraints

The lack of legislation for emergency management is the major regulatory constraint. Most of these constraints will be resolved when the pending National Crisis

Management Center (NCMC) starts its operations. The process of approval for communication equipment and systems still a lengthy one. Another issue is the heavy customs duties currently applicable to emergency/recovery shipments of communication equipment brought into the country.

3. Technical Constraints

The major technical concern is the limitation of resources for training and for retaining qualified communication personnel. Jordan's general communications infrastructure may not be able to readily support the sudden amount of calls in case of a disaster. As in the aftermath of a major disaster, human emotional spontaneous action will be to call their loved ones.

Other technical issues are expected to occur, such as radio communication frequency interference, lack of hotlines and radio links for disaster relief personnel, and lack of communication materials and equipment in case of emergency.

4. Financial Constraints

It is common to suffer lack of funds for emergency management as most agencies will not prioritize fund for something that has not happened yet. Different management parties may allocate different amounts to disaster communication and as such continuity and integrity of emergency services may be compromised.

F. EFFECT OF SEPTEMBER 11 ATTACK ON NEW YORK'S ICT INFRASTRUCTURE

The infamous September 11 attacks provided the U.S. agencies experience resulting in an opportunity for other countries to study and learn. Many agencies and working groups studied the effects of the destruction on the ICT infrastructure.

1. The Communications Infrastructure [9]

The "Lower Manhattan Communication Users' Working Group" issued a report in summer 2002 that contained findings and recommendations for building a 21st Century Communication Infrastructure.

Many of these findings are relevant to the Jordan ICT environment; the report gives a good understanding of the threats and vulnerabilities associated with resilience. The following findings are good to focus on:

1st Finding

"Communications outages after the attacks were a result of an under-appreciation of potential failure points rather than a deficient infrastructure."

2nd Finding

"Local exchange redundancy was not offered as a standard service."

3rd Finding

"Carrier redundancy does not necessarily mean true redundancy."

4th Finding

"The 'last mile' (between local exchange and customer premises) is the key to the resilience of business communications network."

5th Finding

"Property owners and building landlords play a key role in providing communications reliability."

The "Lower Manhattan Communication Users' Working Group" is a telecom industry group which is mainly a Circuit-Switching (CS) technology. Over-centralization causes major disruption in Plain Old Telephone Service (POTS). In the World Trade Center (WTC), three central offices were destroyed which disrupted the service as expected.

BellSouth Phone Company (as an example) reported a three-fold increase in traffic that morning, so phone lines were busy for both cell phones and landlines.

2. The Internet Infrastructure [45]

Tuesday 9/11 2001 was the first real test of the Internet from different perspectives. During and after the event, the Internet proved itself as a vital means of communications. People could not reach anyone on their home phone, cell phone, or work phone, so E-mail ended up being the a successful option.

According to Keynote Systems Inc., an Internet performance measurement company, the Internet's central backbone performed well overall. The Internet showed better resilience, as in the hours following the attack, Internet traffic slowed the major news web sites, and web masters solved that problem by disabling video streaming and graphics from their sites to allow users to access the news faster. Normally, CNN.com gets 14 million page views per day, that morning it reached 9 million page views per hour. ABC news took measures including borrowing server capacity from a sister company at ESPN.com.

Most of the Internet infrastructure, even in lower Manhattan, continued to function normally for two reasons: First, Internet infrastructure is decentralized with no single point of failure. Second, most of Internet Service Providers (ISPs) infrastructure in Manhattan was not within the disaster footprint, which allowed New York Stock Exchange (NYSE) to reopen the following week.

G. SUMMARY

The main goal of this chapter was to explore the U.S. experience in disaster management and interoperability for emergency plan enhancement in Jordan. The main point to take out of the U.S. experience is not to fall into the same mistakes and confusions.

IV. EMERGENCY COMMUNICATIONS INTEROPERABILITY PLAN REQUIREMENTS SURVEY

The resilience of communications infrastructure is vital to the well-being of any country; however, 100% resilience is impossible. Risk management for the probability of communication failure required and appropriate measures to ensure that communication systems are robust and available in case of emergency are always difficult to achieve.

In this chapter, the requirements for the emergency communications interoperability plan are surveyed. To prepare for the disaster, a thorough analysis of the communications infrastructure is required to determine the weaknesses and strengths and feed this information into an asset database which will be used for planning. Single points of failure should be identified and resolved in a timely manner.

A. REQUIREMENTS FOR A PUBLIC SAFETY NETWORK

The First Responders Community (FRC) is used to having its own non-commercial ICT networks in which they do not compete with other users, have priority access, and good security. The requirements for a viable emergency communication interoperability plan could be outlined in accordance with certain headlines: Availability of the infrastructure, security, Quality of Control (QoS), and the ability to reach to mobile platforms. In the following discussions, the approach for the communication infrastructure study is presented.

1. Availability A_o [1]

Availability identifies if the service provider will be able to offer communications continuously in a given area. There are three principles of high availability engineering: Elimination of single points of failure, reliable crossover, and swift detection of failures.

Availability depends on the type of service and the service provider. Availability engineering is needed to create a reliable system and infrastructure. Availability refers to how much time the system takes to be fixed and is up and running again.

In contrast, reliability refers to whether or not the infrastructure is working, and capability is the sum of services provided for the First Responders Community (FRC), and scalability refers to how well the system handles surge conditions, whereas survivability measures the resistance of the system to failure, and finally, there is restorability which is a measure of how easy the system is restored upon failure.

To reduce frequency of failure alone will not increase availability. It should be accompanied by a reduction in the repair time. To design for availability, the system should predict, detect, and resolve the failure (software or hardware) before the system halts, thereby minimizing downtime.

Network availability is vital for the successful accomplishment of various people working in their tasks. Failure of the network stops the overall operation and is not acceptable. Building networks with high availability is feasible using Commercial-Off-The-Shelf (COTS) technology which makes it easier and cheaper for the implementation of survivable information systems. Operational availability (A_o) may be defined as:

$$A_o = \frac{\text{up time}}{\text{total time}} \qquad (1.1)$$

Networks are comprised of components with different availability characteristics connected together. Figure 6 shows an example of a typical network which shows how components affect each other and the outcome of total availability of the information system.

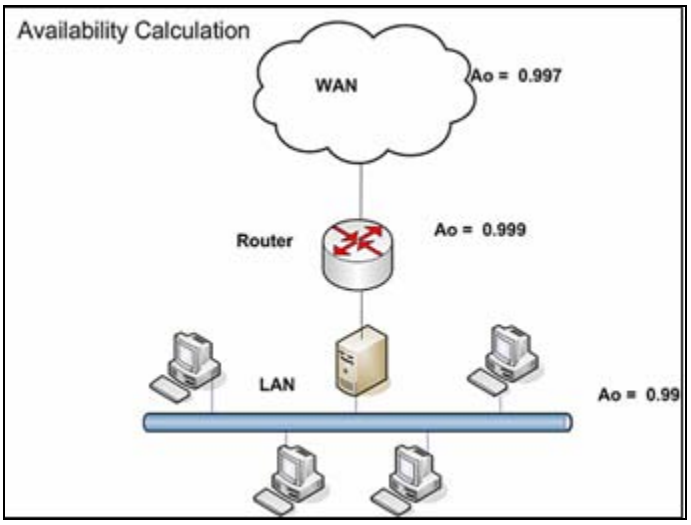

Figure 6. Availability calculation example without redundancy (After: [1]).

As shown in Figure 6, A_o is assumed as 99.7% for Wide Area Network (WAN), 99.9% for the router, and 99% for LAN and end systems collectively. Since these components are connected in a series, A_o total is the product of the A_o for the three components:

$$A_o = 0.997 \times 0.999 \times 0.99 = 0.986$$

For a 30-day month, there are $30 \text{ days} \times 24 \text{ hours} \times 60 \text{ minutes} = 43200 \text{ minutes}$, thus the down time is calculated to be 605 minutes. This is a considerably long down time per month. Redundancy is the best technique to solve this problem High availability requires that a single point of failure be resolved, providing that reliable connection between the primary system and the backup system.

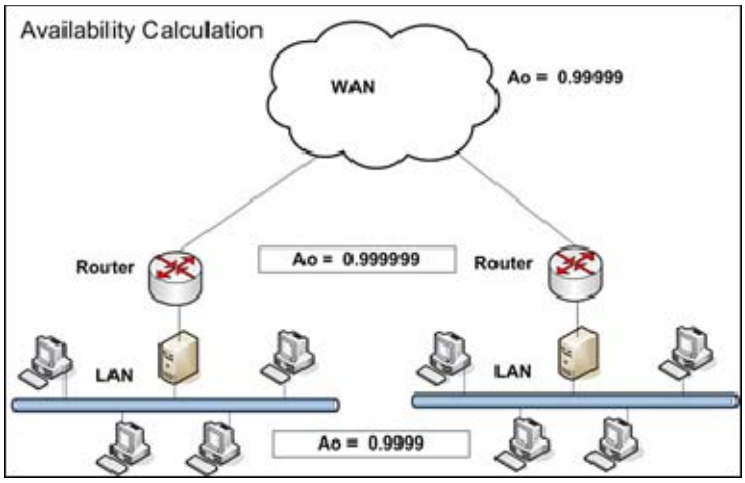

Figure 7. Availability calculation example with redundancy (After: [1]).

In this configuration, $A_o = 0.999889 =$ 5 minutes down time, which is a big improvement toward high availability of the system.

The importance of these values depends on the mission of the system. In the case of mission critical systems, such as 9-1-1 emergency systems, the extra cost of building a redundant system is justified. A comparison of typically used percentages is shown in Table 2 below.

It is important to know that this is not just an emergency services exercise. The infrastructure which is built for emergency services is (and should be) used by day-to-day government personnel including their ability to reach the public. Emergency services properly represent the most demanding requirements for the Internet infrastructure. An example of this could be for the schools to be the backbone of the network in case of emergency.

A robust infrastructure meets the three principles of high A_o engineering: elimination of single points of failure as shown above, redundancy through the infrastructure should solve this issue [8].

Serial	Percentage Quoted	Unavailability (Not usually quoted)	System Unavailability	Typical Example
1	90%	10%	36.5 days/year	Mail server
2	99%	1%	3.65 days/year	Web server
3	99.9%	0.1%	8.8 hours/year	A good ISP
4	99.99%	0.01%	53 minutes/year	GPS
5	99.999%	0.001%	5 minutes/year	UK PSTN
6	99.9999%	0.0001%	32 seconds/year	

Table 2. Comparison of System Availability Data (From: [8]).

The requirements for commercial network availability are not so high, and interruption is not a surprise. Mobile networks enhance the availability of the system by doubling the number of critical components and equip the switches and the base stations with extra batteries.

2. Quality of Service (QoS) vs. Quality of Service (qos) [1]

Quality of Service (QoS) is the quality of service control of configuration to optimize other features. Congestion in the network leads to a requirement to control QoS. Technologies vary regarding the ability to control QoS: WiMAX has the ability to control QoS; while WiFi does not have any significant ability to control QoS. In the wired part of the Internet, implementation of QoS measures is avoided by over provisioning.

The Internet Engineering Task Force (IETF) defines quality of service (qos) (lower case notation) for the qos in the context of how it was experienced. To measure qos there are some factor such as Bandwidth efficiency (throughput), determinism, latency, jitter, and interactivity. Throughput is measured by packet per second; while latency is the time is taken for a packet to get through a network. Jitter is the time of delivery of packets from a source to a receiving system. These factors are dependant on each others. An example for this concept is that WiFi and WiMAX qos behavior (at layer 2) are as shown in Table 3.

	WiFi	WiMAX
Bandwidth efficiency	Contention MAC (CSMA). This means that bandwidth efficiency is very low (about 20% of the baseband capacity of the channel).	Non-contention MAC. This means that bandwidth efficiency is very good (about 90% of the baseband capacity of the channel).
Determinism	There is no determinism. There is a probability that the packet will get accepted, but no tight assurance and no assurance within a bounded time window.	Determinism is good. Once an SS is in the network, it is assured a transmit window within a finite amount of time.
Latency	Good latency only in a lightly loaded network.	Latency and interactivity are traded off.
Jitter	Good latency only in a lightly loaded network.	Good jitter as it is based on determinism.
Interactivity	Good latency only in a lightly loaded network.	Latency and interactivity are traded off.

Table 3. WiFi and WiMAX qos behavior (From: [1]).

3. Security and Privacy

Security is categorized into two parts: content protection and infrastructure protection. Content protection includes authenticity, confidentiality, integrity, and non-repudiation quartet.

Infrastructure protection includes resistance to Denial of Service (DOS) and Type of Service (TOS) attacks, resistance to Threat Analysis (TA) /Two Factor Authentication (computer security authentication) analysis, Low Probability Intercept (LPI), and Transmission security (TRANSEC) issues. It is a common mistake to attempt to use remedies targeted at infrastructure protection problems at the content protection problem [1].

The network should offer high level of identification and authentication for users to limit fraudulent access and data interception. Different types of encryption are also

necessary to enhance privacy. Compromise is necessary between security measures for public safety network and accessibility so that it will be closed for the public in case of emergency.

If the First Responders Community (FRC) is to share an open commercial network with other users, they should enjoy the same security as they have in current private networks. Groupe Spécial Mobile (GSM) networks do not include end-to-end encryption, GSM telephones that are safe from eavesdropping have been launched, but they are expensive.

B. NETWORK ATTRIBUTES

1. Coverage

Coverage identifies whether users can use the wireless network in a particular area. Typically, service providers focus on coverage in high population area, which means that rural areas may not have full coverage. Some factors may affect the coverage level: power of transmission, structures and obstacles in the area, and the frequency used.

The First Responders Community (FRC) requires coverage of all of the geographical areas of the country. GSM networks usually do not have coverage outside populated areas due to its user-based business model. GSM coverage in Jordan is estimated to be around 65% [46].

2. Accessibility

Accessibility is how readily users can access and utilize the wireless network. Accessibility is important during peak hours and network disruption as those circumstances coincide with disasters and emergencies.

It is vital to make government infrastructure services more accessible to citizens and other clients. A key is to leverage services between country agencies, central and local government and to promote inter-agency and inter-governmental data sharing [7].

3. Transmission Speed

The transmission speed is defined as the rate at which data is transmitted through the network. There are factors that affect the rate of transmission such as error correction technique used, level of traffic on the network, and bottlenecks between components of the network [7].

4. Fast Call Setup

Fast call setup is the time that the system needs to put on a call and is important, especially in the case of emergencies.

The First Responders Community (FRC) requires a call setup of below 1 second with call length of several seconds. GSM is intended for commercial use with users having a different usage profile where a call setup is about 3 seconds with call length of several minutes [20].

Reducing the call setup time requires important changes in the commercial mobile network switches. If the backbone is based on Packet-Switching technology and the network is using routers, call setup requires milliseconds only.

Another way to solve the problem would be keeping the channels open on a permanent basis within a cell in case of emergency, which would require an enormous extra capacity.

5. Network Capacity

It is essential to have sufficient capacity, especially in the case of an emergency. The commercial mobile networks have not been built for many simultaneous calls within a limited geographical area (in case of Circuit-Switching (CS) infrastructure) [7].

6. Direct Local Communication

The users within a limited area must be able to talk to each other, even if the network is temporarily out of order. In commercial mobile networks, the calls are directed through the network and cannot be done directly.

The TETRA-handsets are designed to communicate with each other within a limited geographical area, even if the network does not function (direct mode operation).

WiFi and WiMAX have this feature as these network architecture types could enable users to talk to each other locally. Satellite phones do not have this feature as the phones are connected directly to the satellite network [13].

7. Group Communication (Multicast)

The First Responders Community (FRC) tends to talk simultaneously. All users have to be informed all the time (without having to think about whether certain user has been notified). GSM supports broadcast, but not flexible group calling [13].

8. Control Room Solution

The First Responders Community (FRC) has a requirement working in an operation control room where these FRC members work in well-equipped control rooms to control large groups of rescue personnel in the field. Commercial mobile networks do not support this way of working [7].

9. Addressing Functionality

Addressing functionality is defined as the way by which a specific service is accessed; voice services may be accessed in two ways: Push-To Talk (PTT) and touch-tone dialing. FRC members are used to PTT systems [13].

10. Cost

The cost for any system includes its primary cost, the running cost and longer term life cycle (replacement) costs. Affordability of the system is important for the level of its spread and usage. Procurement of new equipment should be decided with respect to the running cost and the salvage value for the systems in service. The decision for the specific infrastructure technology procurement should be made at a high level to lessen the risk that many agencies may procure non-interoperable systems.

11. Mobility

Mobility is a crucial attribute for an emergency response mission. First Responders Community (FRC) members will set up temporary field facilities that require communications and other logistics support. In this case, the easiest way to furnish communication solutions would be wireless connections. While WiFi may be used to connect locally, WiMAX is fit for long haul point to point or point to multi-point purposes.

WiMAX (terrestrial bridging) technology is characterized by swift deployment in harsh conditions to provide reliable voice, video, and data communications for wider distances than other terrestrial wireless technologies [1].

Response to emergency situations is on two levels, local and non-local. Local authorities and groups should have the assets, awareness, and training to react instantly to the emergency. Non-local agencies mean countrywide, private sector, and sometimes those of international domain [13].

C. INTEROPERABILITY REQUIREMENTS

A public safety response to emergencies is based on ICT services. Interoperability is defined as the ability of different agencies to work together which include PTT radios, trunking, and other wireless or radio systems. Capabilities and assets are combined in harmony to reach this goal.

Procurements according to specific interoperability standards builds an interoperable communications network. Currently, communications networks should be routable to be interoperable with each other. There are four communications types needed; each one needs an appropriate amount of attention [1]:

1. Government-Government Communications Needs

Fire departments, as an example, need to talk to each other across jurisdictions and to police departments. An effective dispatching, resilient hardware solution set, and common language are needed.

2. Citizen-Government Communications Needs

Citizens are a valuable source of information to the government. This relationship could be enhanced by promoting public awareness about the importance of their feedback and contributions.

3. Citizen-Citizen Communications Needs

This communications need between citizens was evident in many emergencies such as the December 2004 Southeast Asia tsunami. Another clear example for this need is when a bridge collapsed in the U.S. The I-35 Bridge collapsed in Minneapolis, Mn, USA in the summer of 2007. The collapse was during rush hour, which caused a large missing-persons list and overwhelmed the regions emergency services agencies and personnel. The list was suppressed using the citywide WiFi network which was opened to the public and “I am OK” messages between citizens were transmitted [1].

4. Government/Military-NGO Community Communications Needs

This is specifically true for major international disasters that multiple nations respond to (i.e., Pakistan earthquake). Collaboration and cooperation is enhanced when communications interoperability is better.

D. SUMMARY

Interoperability is vital for First Responders Community (FRC) members on the ground to be able to talk to each other. Currently, many solutions are flooding the market to try to address myriad problems that arose out of these past disasters and incidents. Power is the core of any system to work in this harsh environment with the assumption that the normal electricity grid may be out of order in disaster time.

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMMUNICATIONS TECHNOLOGIES OVERVIEW

In this chapter, overviews for most of the communications technologies standards currently available are introduced. This background is needed to furnish an emergency communication interoperability plan.

Communications technology standards can be generic, open, or proprietary. Generic standards define independent objectives for equipment functions. It allows a design to be either open or proprietary. Open standards use a collaborative methodology which makes system components interchangeable by another vendor. Open standards lead to lower prices, better interoperability, and better performance due to competition. Proprietary standards are often controlled by a specific vendor which promotes a monopoly of their particular solutions and could lead to higher prices than are necessary [13].

Commercial-Off-The-Shelf (COTS) technology allows replacing proprietary network equipment. COTS technology advantages are availability, the ability to introduce new applications in less time at lowered costs, and system interoperability.

A. WIRELINE VS. WIRELESS COMMUNICATIONS MEDIUM

1. Wireline Communications Medium

Wireline communications mediums include copper, coaxial cable, and optical fiber. These wireline communications mediums could be using a Circuit-Switching technology or a Packet-Switching technology.

These wireline communications mediums have advantages such as security, availability, and reliability. Disadvantages for these mediums are the high installation cost, susceptibility to disasters (floods, earthquakes), and lack of flexibility.

2. Wireless Communications Medium

Wireless and radio communications medium refers to the radio frequency (RF) spectrum. Many technologies utilize this medium such as: Satellite, radio & television broadcasting, computer networks, cellular, and Specialized Mobile Radio Technologies [30].

The First Responders Community (FRC) has been the pioneer for the use of wireless data capabilities. Wireless technologies are depicted in Figure 8.

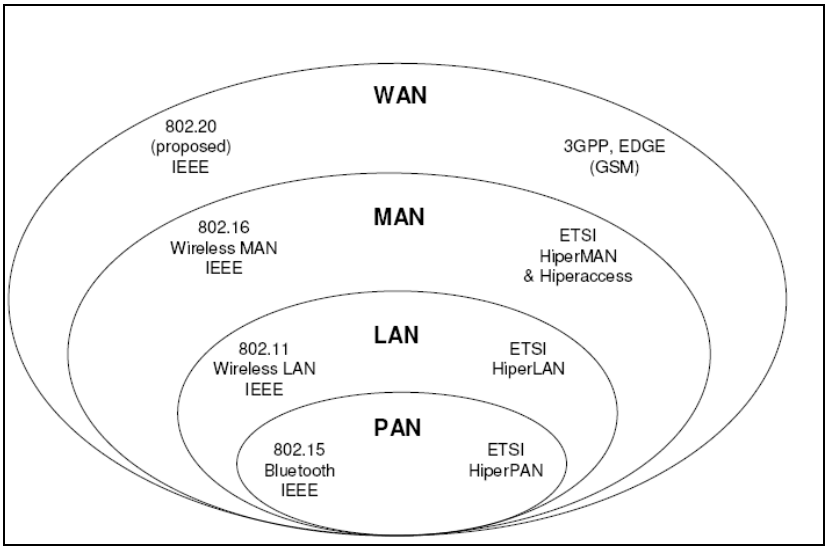

Figure 8. Wireless Standards (From: [30]).

Wireless systems are the essence of mobility which is necessary for public safety applications. These systems provide the required reliability, availability, accessibility, control, security, and functionality to meet the emergency and tactical communication needs of First Responders Community (FRC). Table 4 depicts the characteristics of wireless systems the dominant tool for public safety agencies.

Functional Requirement	Wireless Systems Characteristics
Sufficient coverage to support component missions	Provide coverage in areas of public safety operations Provides in-building coverage
Sufficient availability to support public safety operations	Wireless systems capacity for availability during emergency conditions
Reliable services to ensure support to components missions	Wireless systems provide the reliability and responsiveness needed public safety operations
Ease of addressing and instant communications	Provides instantaneous push-to-talk functionality
Hands-free operations	Provides hands-free functionality for public safety requirements
Components for control critical assets	Provides public safety agencies control of assets, including Over-The –Air Rekeying (OTAR) and Over –The-Air management (OTAM)
Security of communications and operations	Provide high level of security
Non-dependency on commercial assets	Ensure non-dependency on commercial assets that may be vulnerable to attack (physical and electronic)

Table 4. Wireless Systems Characteristics (After: [21]).

B. CIRCUIT-SWITCHING TECHNOLOGIES OVERVIEW

Circuit-Switching (CS) technologies are still in use even if efforts are continuing toward transforming to Packet-Switching (PS) technologies and applications. The following is an overview of the most important Circuit-switching technologies:

1. Satellite Technology

Satellite technology plays a vital role in all human life aspects. There are three popular satellite orbits [19]:

a. Low Earth Orbit (LEO)

LEO orbit is located at 1,250 miles above earth and it takes the satellite 90-120 minutes to rotate around earth.

b. Medium Earth Orbit (MEO)

MEO orbit is located at 6,250 miles above earth and it takes the satellite 6 hours to rotate around earth.

c. Geosynchronous Orbit (GEO)

GEO orbit is located at 22,282 miles above earth and it takes the satellite 24 hours to rotate around earth.

Mobile satellite services are useful for the First Responders Community (FRC) as it can connect them almost anytime and anywhere on the globe. Satellite technology is not as vulnerable to physical damage as other types of networks - making it relatively more reliable than other technologies. Figure 9 depicts typical satellite solutions for communications in emergencies. Fixed, handheld terminals are examples of satellite solutions.

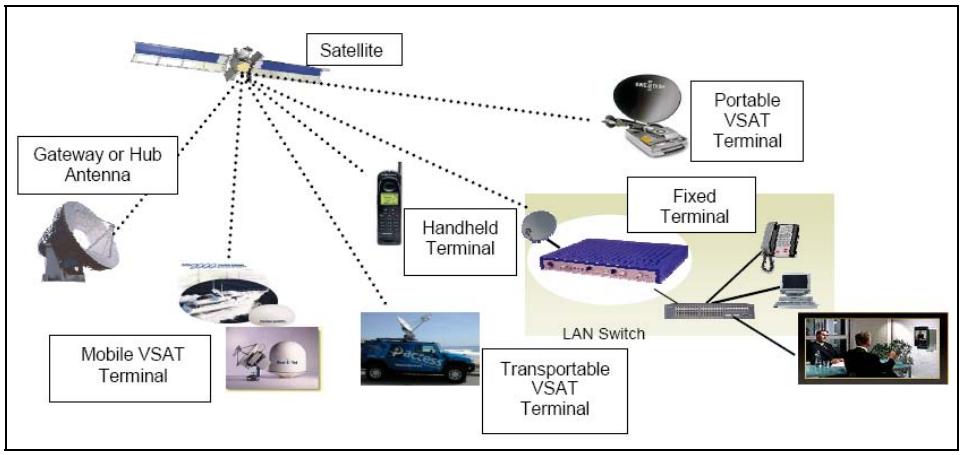

Figure 9. Satellite Solutions for emergency communications (From: [5]).

Most mobile telephone networks operate close to capacity during normal times. Large spikes in call volumes caused by widespread emergencies often overload the system just when it is needed the most. Examples reported in the media such as: the attacks of 9/11/2001, the December 2004 Southeast Asia tsunami, the 2003 Northeast (U.S.) utility grid power blackouts, Hurricane Katrina, and the 2007 Minnesota bridge collapse.

Also, terrestrial cell antennas and networks are vulnerable to natural disasters. Satellite telephony can usually avoid this problem in communications during

natural disaster. Satellite phones usage is popular for expeditions into remote areas where terrestrial cellular service is unavailable. Following are common technologies in this domain:

2. Satellite Vendors

a. Broadband Global Area Network (BGAN)

BGAN is an L Band satellite Internet and telephony network provided by INMARSAT. The system uses two geostationary satellites; with a third satellite launched in August 2008 and expected to be in service in early 2009. The system will then cover all parts of the world except for the highest portions of the Polar Regions.

The advantage of BGAN over other satellite systems is that the terminal is portable, easy to use, and has high of quality and speed for both voice and data services. The system utilizes the L band, which is more resistant to rain fade than most other satellite frequencies.

b. Thuraya [47]

Thuraya (the Arabic name for the Pleiades) is a regional satellite phone provider. Its coverage area extends to most of Europe, the Middle East, North, Central and East Africa, Asia and Australia.

The company is based in the United Arab Emirates (UAE) and distributes its products and services world wide through authorized service providers. The current number of subscribers in the network is around 250,000 (March 2006).

The system offers voice communications with handheld or fixed terminals, Short Message Service (SMS), and 9.6 Kbit/s of data & fax service. GPS is supported by all handsets.

c. Iridium [48]

The Iridium satellite system is a constellation of 66 active communication satellites with spares in orbit and on the ground. It allows worldwide voice and data communications using handheld satellite phones.

The Iridium network is unique in that it coverage extends to the whole earth, including poles, oceans and airways. The company claims to have 285,000 subscribers (August 2008).

Despite the bandwidth limitations, transparent IP is supported. Iridium claims data rates up to 10 kilobits per second (kbps) for their "direct Internet" service.

An evaluation of this technology for emergency communications could be derived. It proves that it is currently the most reliable and dominant in the field of emergency relief and response, especially in the international domain. Satellite communications technologies in general are Hastily Formed Network (HFN) enabled, mobile and usage flexibility is one of its strongest attributes.

2. Mobile Telephony

Throughout all other technologies, the merging of mobile telephony and the Internet were the two biggest successes. Currently, mobile handsets in some countries are more than fixed phone lines. Following an overview of the mobile telephony evolution [35]:

a. The First Generation (1G)

The first generation (1G) of mobile telephony used analogue communications such as the following standards: The first cellular network standard Advanced Mobile Phone System (AMPS), Total Access Communication System (TACS) is the European version of the AMPS standard, and Extended Total Access Communication System (ETACS), which is an enhancement of the TACS standard. Figure 10 depicts the evolution of mobile telephony standards [35].

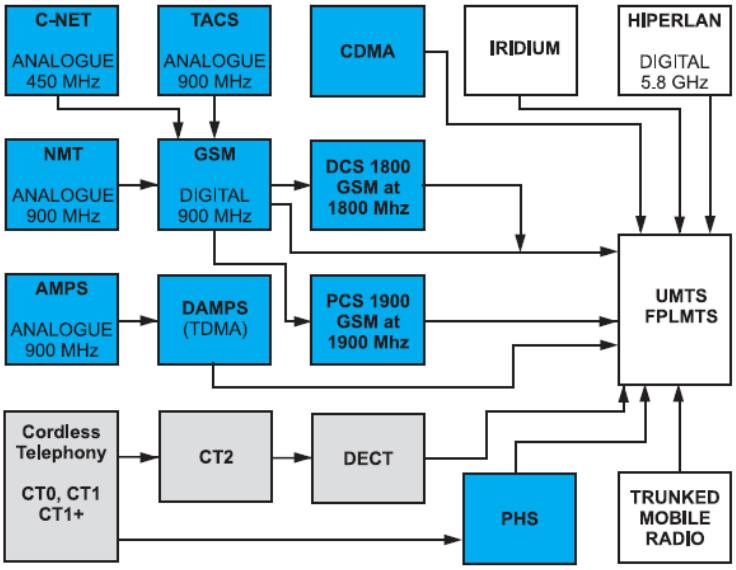

Figure 10. The mobile technology evolution (From: [20]).

b. The Second Generation (2G)

The second generation (2G) of mobile networks switched from analogue to digital communications, the following standards are examples: Global System for Mobile communications (GSM) or Groupe Spécial Mobile (GSM), Code Division Multiple Access (CDMA), and Time Division Multiple Access (TDMA).

2G was enhanced to 2.5G as General Packet Radio System (GPRS) standard and 2,75G as the Enhanced Data Rates for Global Evolution (EDGE) standard.

GSM is discussed in more detail in the following section as it is the most successful standard in mobile telephony.

(1) Groupe Spécial Mobile (GSM)

In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to develop a mobile telephone system.

The European Telecommunication Standards Institute (ETSI) took over the project and published the first specification in 1990. While data services are available,

typically at 9.6 kbps the primary use of GSM is for voice. GSM cells are limited to approximately 35km diameter. GSM is the dominant cellular technology worldwide [46].

In circuit-switched systems, QoS is binary (either the call gets through or not), but when overloaded, the system will be jammed and no services are offered which was a big flaw [1].

Coverage and availability are almost tied together but sometimes a call cannot be completed in a service area due to the lack of capacity of the network. Other factors that can limit availability include the level of area priority, Radio Frequency (RF), and terrain characteristics.

GSM network call dropouts are often due to power loss in the area and handover failure. Transmission quality measurements start once the call is established which includes low voice volume, level of noise, echo, crosstalk, and garbling (breaking-up). Post Dial Delay (PDD) is the time the GSM network takes to initiate a call. Mainly, this factor depends on how fast the network is able to route a call.

GSM Quality of Service (QoS) is based on call procedures and voice criteria as data is still limited on GSM network. The parameters which could be tested in context of QoS are coverage, availability, call dropouts, transmission quality, and Post Dial Delay (PDD).

In emergency response, a mobile network cell can be installed on location and cell phones can quickly be disseminated to users. A satellite link is used as a back haul and may be used in international deployment for First Responders Community (FRC) members. The services of cellular technology will be useful for the users, which are not available in other solutions such as messaging, multimedia sharing, and location.

The evaluation for cell technologies is based on the fact that it is not based on a routable network. The case should be made that those new technologies using cellular infrastructure with IP based applications are evolving [1]. Table 5 shows the typical attributes for mobile telephony standards.

Generation	Standard	Description	Data Rate (Kbps)	Throughput (Kbps)
2G	GSM	Transfer voice, or low-volume data	9.6	9.6
2.5G	GPRS	Transfer voice, or moderate-volume data	21.4-171.2	48
2.75G	EDGE	Simultaneous transfer voice & data	43.2-345.6	171
3G	UMTS	Simultaneous transfer voice& high-speed data	144-2000	384

Table 5. Mobile Telephony Standards (From: [35]).

c. The Third Generation (3G) [49]

Third generation offers a set of new technologies that offers true mobile, broadband data: video on demand, videophones, broadband gaming, real-time audio, and other broadband services. 3G standard are Universal Mobile Telecommunications System (UMTS), and High-Speed Downlink Packet Access (HSDPA) sometimes categorized as 3.5G.

d. The Fourth Generation (4G)

Fourth generation (4G) is the future of cellular technology which looks promising in the context of interoperability. The first generation (1G) and second generation (2G) systems were mainly designed for voice telephony transmission. The third generation (3G) is for both voice and data transmission but still not routable network and it is point-to-point [1].

The fourth generation (4G) is still in the planning stages and needs more years to be fully deployed. The expected timeframe for full 4G implementation is about 2012-2015 where systems should be interoperable with existing wireless standards.

While 3G systems are based on two infrastructures in parallel consisting of Circuit-Switching and Packet-Switching network nodes, the target for the 4G systems

is an IP, packet switched network solution where voice, data and streamed multimedia are available "Anytime, Anywhere" for users along with higher data rates than previous generations.

In 4G systems, Internet Protocol version 6 (IPv6) support is essential in order to furnish service for a large number of wireless-enabled devices. IPv6 also enables a number of applications with better multicast, security, and route optimization capabilities.

The technologies which are being considered as pre-4G are the following:

(1) Fast Low-latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing (Flash-OFDM) which is also referred to as F-OFDM, is a system that has generated interest as a packet-switched cellular bearer [50].

(2) WiMAX. Worldwide Interoperability for Microwave Access (WiMAX) forum is a non-profit industry organization formed to emphasize the adoption of this technology to assure interoperability between different vendors' products.

(3) WiBro (Wireless Broadband) is the South Korean service name for the IEEE 802.16e (mobile WiMAX) international standard [34].

(4) iBurst or High Capacity Spatial Division Multiple Access (HC-SDMA) is a wireless broadband technology that optimizes the use of its bandwidth with the help of smart antennas [49].

(5) 3GPP2 Ultra Mobile Broadband (UMB) was the brand name for a project within 3GPP2 to improve the CDMA2000 mobile phone standard for next generation applications and requirements [51].

(6) The Third Generation Partnership Project (3GPP) started the Long Term Evolution (LTE) project to improve the Universal Mobile Telecommunications System (UMTS) mobile phone standard to cope with future technology evolutions. Goals include improving spectral efficiency, lowering costs, improving services. While 3GPP Release 8 has yet to be ratified as a standard, much of the standard will be oriented around upgrading UMTS to a 4G mobile communications technology [49].

A large amount of the work is aimed at simplifying the architecture of the system, as it transits from the existing UMTS circuit & packet switching combined network, to an all-IP flat architecture system.

The main benefit of 4G systems for public safety communications is interoperability as it will seamlessly hand-off the user from one network to another even with different frequencies and technologies.

3. Land Mobile Radio Systems (LMRS) Standards [36]

Land Mobile Radio Systems (LMRS) standards include public safety and specialized mobile radio technologies standards which are designed for public safety communications.

These communications standards could be open or vendor-proprietary. The following standards are considered as open: TETRA of European Telecommunications Standards Institute (ETSI), TETRAPOL (TETRAPOL Forum). The following standards are considered as proprietary: iDEN of Motorola, EDACS of Ericsson.

Trunking is characterized by having a controller in the network that maps and assigns calls to channels. Conventional systems repeat radio calls from one frequency to another. To accommodate a very large number of subscribers, trunked radio systems typically allocate more frequency pairs (channels).

Trunked radio system is a radio topology intended to create an efficient frequency spectrum network. One of the advantages for trunked radio systems is that each agency can separate its communications by having a talk group. Another advantage to a trunked system is the increased immunity against eavesdropping as the system switches channels many times during a communications session. The main disadvantage of the trunked system is the complexity of the infrastructure.

Figure 11 depicts the evolution of public safety radio standards. The figure shows two main tracks: U.S. and European technologies.

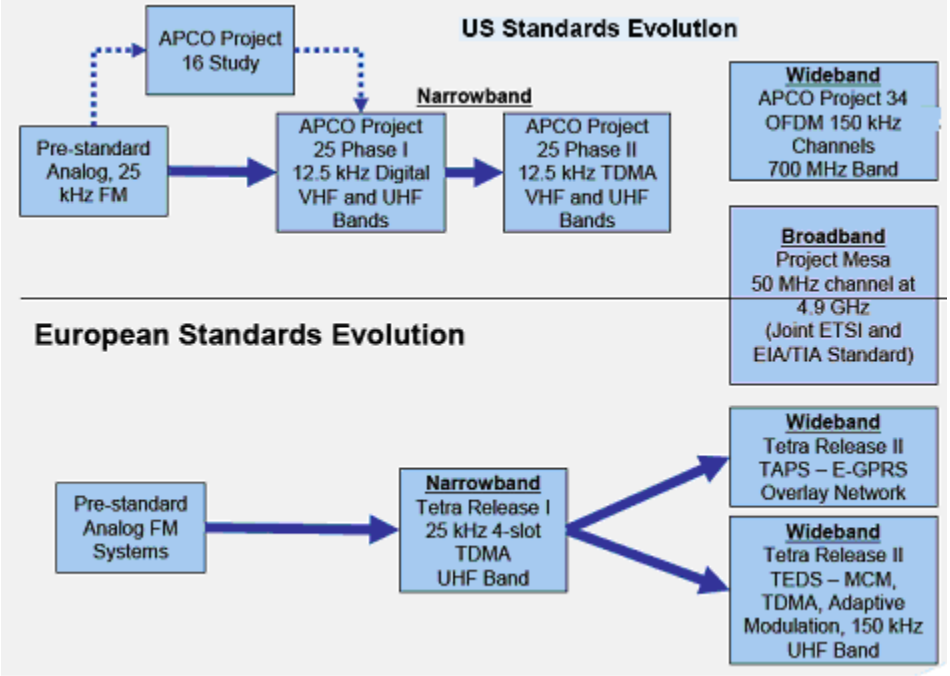

Figure 11. Evolution of Public Safety Radio Standards (After: [36]).

The Association of Public Safety Communications Officials International (APCO) started several projects toward trunking technology standardization. APCO Project-16 (P16) is a project that was developed in the 1970s as a standard for analog trunked radio systems. This standard was adopted by public safety agencies and industrial users.

APCO and National Association of State Telecommunications Directors (NASTD) started P25 in 1989 as a result of P16 incompatibility. The aim of the project was a standard which would provide interoperable emergency communications.

Project 34 (P34) is a EIA/TIA standardized system for provision of packet data services in an interoperable dispatch oriented topology for public safety service providers

In this thesis, TETRA & iDEN are discussed in detail as they are already installed in Jordan. The GSM Trunking System (GSMT) is also elaborated upon as an interoperability technological solution:

a. Integrated Digital Enhanced Network (iDEN/Motorola)

iDEN is a Motorola proprietary standard for mobile phone system (push-to-talk radio dispatch messaging, and data communication). It is based on TDMA technology with (800) MHZ frequency band (1.5 GHZ in Japan) [23].

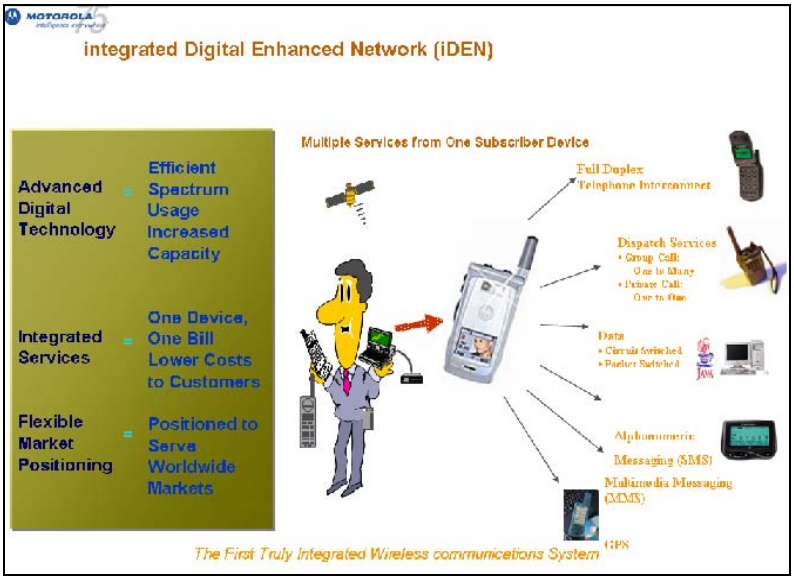

Figure 12. iDEN System Services (From: [26]).

b. Terrestrial Trunked Radio System (TETRA)

TETRA is sometimes called Trans-European Trunked Radio System (TETRA). This standard was defined by the European Telecommunications Standards Institute (ETSI) for the Private Mobile Radio (PMR). Public safety and emergency services are embedded in the core design of this technology as it offers bandwidth-on-demand, unlimited group size, priority calls, call pre-emption, and all-informed communications [24].

The first agencies to implement TETRA were the European public safety and emergency services (Police, Medics, and other related groups). A comparison between Private Mobile Radio (PMR) and Public Communication Network (PCN) is elaborated upon in Table 6.

	Private Mobile Radio (PMR)	**Public Communication Network (PCN)**
Traffic Density	Low to Medium	Medium
Call Setup	Fast push-to-talk of 300 msec	Interconnection time about 5 msec
Call Duration	About 20 Sec, High Frequency	2 Minutes
Call Profile	90% made within same region, 60% initiated by control dispatcher	85% made via PSTN, 5% mobile to mobile in different region and 10% mobile to mobile in same region

Table 6. Differences Between PMR and PCN (After: [38]).

TETRA is a Time Division Multiplexing Access (TDMA) narrowband system (25 KHz) using 4-slot TDMA to provide digital voice and data services for up to 4 simultaneous users. The main difference between TETRA and GSM is the usage scope. TETRA is designed for professional applications while GSM is designed for public telephony. A comparison between iDEN and TETRA is elaborated upon in Table 7 [24].

	Peak Data Rate	**Max Range (Km)**	**Duplexing Approach**	**Channel BW**	**Duplex Spacing**	**Applicable Band**
iDEN	36 kbps	3.8-17.5	FDM	25 KHz	45 or set by regulator	870-888/915-933 or set by regulator
TETRA	64 kbps	5-40	FDM	25KHz	45KHz	800/900 MHz

Table 7. TETRA vs. iDEN Comparison (After: [24]).

When the trunked radio is built, it is vital to assure First Responders Community (FRC) members' connectivity to a citizen on any other network such as the Internet. The GSM interconnection to this closed network may be facilitated using GSMT technology discussed below. On the other hand, WiMAX and WiFi may be used to connect LANs infrastructure to the nation-wide infrastructure.

c. GSM Trunking System (GSMT) [38]

GSMT supports all standard GSM services in addition to trunking services as shown in Figure 13.

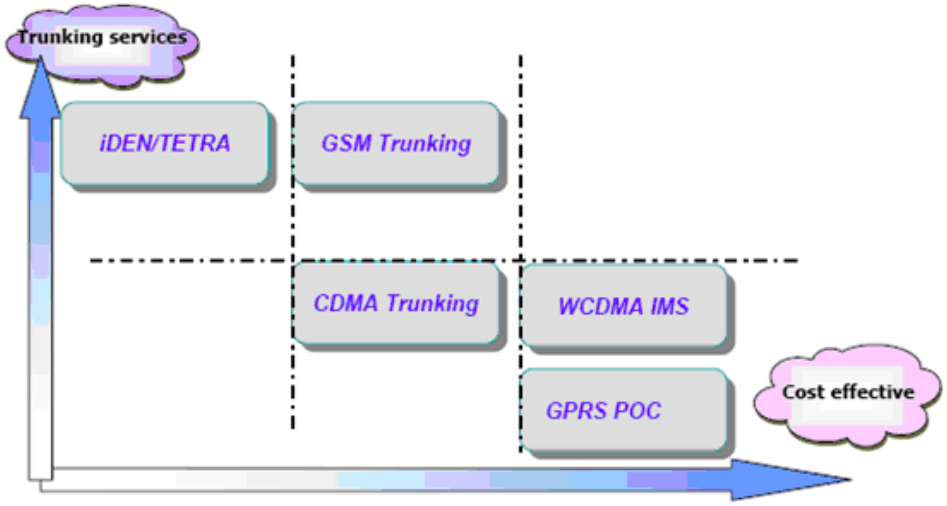

Figure 13. GSMT Evolution (From: [38]).

GSM has a little performance degradation due to more nodes and signal procedure complexity. As GSM is cost effective, some operators in Europe are cooperating with governments for trunking over GSM. GSMT aims to maximize service availability, efficiency, security, and dispatching convenience.

	iDEN/TETRA	**GSMT**
Performance	High Performance Call Setup time less than 500 ms PTT time less that 300 ms	Similar performance Call setup time less than 1 s PTT time less than 300 ms
Service	Trunking service+ poor data service	Trunking service+ All GSM service
Cost	High cost	Cost effective
standard	Private	To be standardized
Roaming	No	Yes
Evolution	Limited	To 3G (dual mode)

Table 8. TETRA/iDEN vs. GSMT Comparison (After: [38]).

C. PACKET-SWITCHING TECHNOLOGIES OVERVIEW

There are several Packet-Switching technologies in use, but the following is an overview of the relevant ones to this thesis:

1. Satellite Technology: Satellite Internet Access

Due to it high cost, usually, users choose satellite technology solutions due to unavailability of other cheaper services. Other reasons may be that local infrastructure is very expensive. There are two main types of Satellite Internet service: two-way and one-way.

Two-way satellite Internet service includes sending and receiving data from the remote Very Small Aperture Terminal (VSAT) site via satellite to a hub. The hub then relays data through the Internet. The satellite dish at each location must be precisely pointed to avoid interference with other satellites.

Almost all VSAT systems are IP-based technology, with diverse applications. Data rates typically range from narrowband up to 4 Mbit/s [54].

2. IEEE 802.11 Standard

The IEEE 802.11 based suite of standards is for Wireless Local Area Networks (WLAN). The IEEE 802.11 standard was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in 1997, which provides data rates of 1 Mbps and 2 Mbps [14].

The Wireless Fidelity (WiFi) term was originated with Wireless Ethernet Compatibility Alliance (WECA), an organization standardizing the development and applications of IEEE 802.11 compliant products.

Channel Number	Frequency GHz	North America	Europe	Spain	France	Japan MKK
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

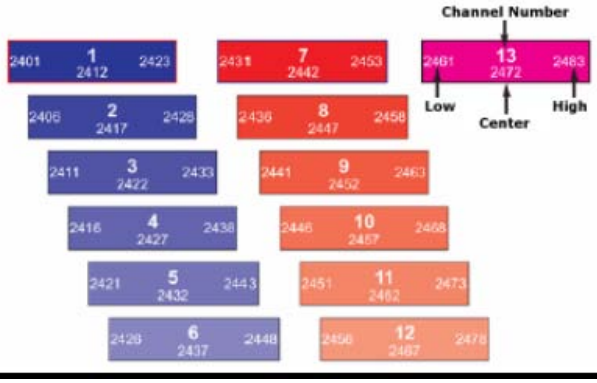

Figure 14. 802.11 Frequency Spectrum (From: [17]).

Normally, a WiFi network includes an Access Point (AP) and wireless clients connect through it. The AP beacons its Service Set Identifier, Network (SSID) name every 100ms.

Advantages of WiFi are: uses unlicensed radio spectrum, allows easy LAN deployment, reduced cost as it does not use cables, and supports various degrees of encryption to protect traffic from interception.

The disadvantages of WiFi are: Limited level of mobility, vulnerable to interference, designed technically for short-range operations and it is basically an indoors technology, and there are still security issues to be addressed [17].

WiFi uses Wired Equivalent Privacy (WEP), also known as Shared Key Authentication, as an optional security measure. WEP was developed to protect the wireless.

Newer security standards for WiFi were introduced in response to several serious weaknesses found in WEP such as: WiFi Protected Access (WPA) which use better security protocol named Temporal Key Integrity Protocol (TKIP), WiFi Protected Access 2 (WPA2) which uses Advanced Encryption Standard (AES) block cipher as a replacement for the Ron's Code 4 (RC4), WiFi Protected Access with Pres-shared key (WPA-PSK) and Robust Security Network (RSN) which uses AES Encryption [17].

An evaluation of WiFi technology for emergency communications could be derived. WiFi is Hastily Formed Network (HFN) enabled; ease of usage is a key feature. Its lack of security is normally not an issue here as it is often not a priority as access to the network in case of emergency is often deemed to be wide open.

3. IEEE 802.16 Standard

The 802.16 standard was specified by the Institute of Electrical and Electronics Engineers (IEEE). Worldwide Interoperability for Microwave Access (WiMAX) is the industry association. These entities overlap, but they are different (similar to IEEE 802.11 and WiFi overlap) [1].

The WiMAX forum is a non-profit industry organization formed to emphasize the adoption of this technology to assure interoperability between different vendors' products. WiMAX Forum Certified™ signature on equipment means that it has been tested and shown to be following the standard. The user may procure from multiple vendors with no compatibility concerns. In this thesis, the WiMAX term will be used whenever possible.

WiMAX can support two forms of wireless service: Non-Line Of Sight (Non-LOS) form and Line Of Sight (LOS). Non-LOS works in the same manner as WiFi systems where an antenna on a computer connects to the WiMAX tower. It uses a lower frequency range (2 to 11 GHz) [2].

LOS uses a fixed, high antenna that must point straight at the WiMAX tower and match up with its antenna. LOS has better and robust performance. It uses higher frequencies — up to 66 GHz with coverage area of up to 30 miles in ideal conditions.

Due to the flexibility and high performance of WiMAX, on July 22, 2006, it was reported that the first deployment of a WiMAX multipoint network at sea of eleven off-shore oil rig platforms in the Gulf of Mexico, USA. This network used 3.4 GHz WiMAX transmissions with double redundancy components and systems at all locations with span average of 10 Km [27].

The following figure depicts WiMAX subscribers forecast until 2012. The figure shows that mobile WiMAX will be dominant in the future.

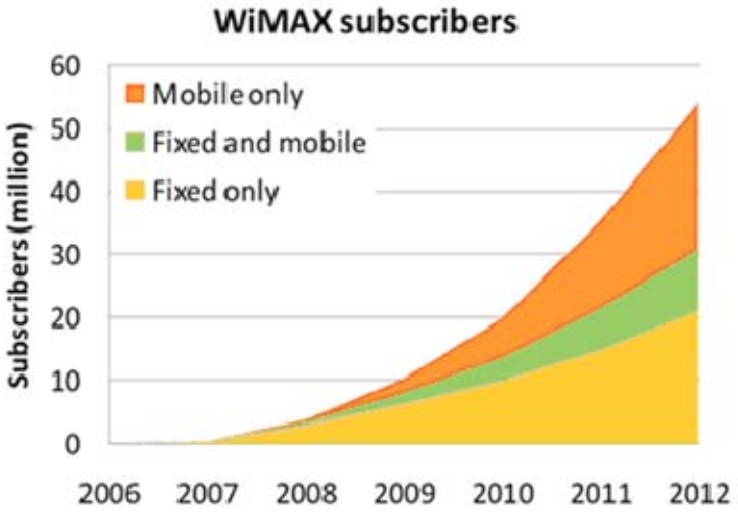

Figure 15. WiMAX Subscribers Forecast (From: [34]).

a. Fixed-WiMAX

802.16-2004 (often referred to as 802.16d) is designed to allow users to access the service from various locations covered by the network. Currently, as there are no portable devices, users can access the service only from their home location, where the Customer Premises Equipment (CPE) is installed. IEEE 802.16-2004 represents a turning point where compliant products started to appear. It uses selectable channel bandwidth from 1.25 to 20 MHz. Customer Premises Equipment (CPE) comprises of outdoor directional antenna and indoor modems.

802.16-2004 is a cable replacement business model, where WiMAX equipment is used as a radio-WAN cloud with routers at the border. WiMAX can reach

mobile platforms and be a bridging backbone for WiFi systems. In remote areas without infrastructure, connecting using WiMAX technology is almost always cheaper than wireline technologies [1].

Mobility (m) version will be IEEE 802.16-2008 or IEEE 802.16-2009 versions. Figure 16 depicts the evolution WiMAX standards.

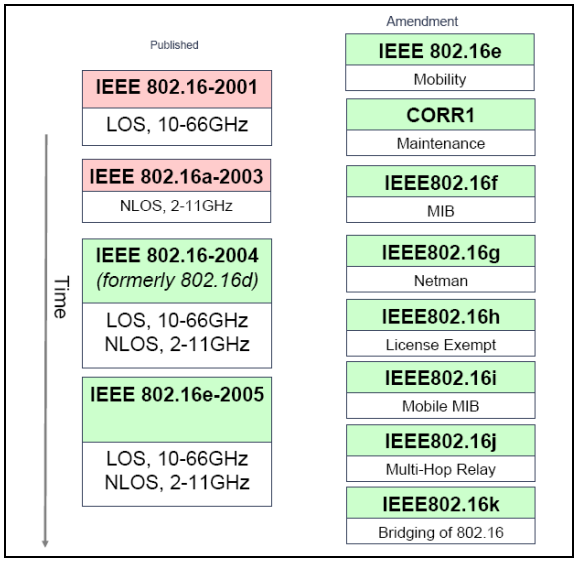

Figure 16. WiMAX Evolutions (From: [31]).

b. Mobile-WiMAX

802.16-2005 (often referred to as 802.16e) adds mobility to the WiMAX. Seamless handover and roaming is feasible when users are moving from cell to cell. Vendors planned WiMAX chips to be installed as PC data cards, mobile handsets and laptops. 802.16-2005 allows mobile wireless broadband access at vehicular speeds. Customer Premises Equipment (CPE) comprises of PC data cards, laptops, and mobile handsets with embedded WiMAX chips. 802.16-2005 is a cell phone replacement business model, where this model needs handoff technique labeled (mobility enhancements). Comparison between WiMAX standards is depicted in Table 9 [27].

	802.16	802.16a	802.16-2004	802.16-2005
Time Frame	December 2001	January 2003	June 2004	December 2005
Spectrum	10-66 GHz	< 11 GHz	< 11 GHz	< 6 GHz
Operation	LOS	Non-LOS	Non-LOS	Non-LOS and Mobile
Bit Rate	32-134 Mbps	Up to 75 Mbps	Up to 75 Mbps	Up to 15 Mbps
Cell Radius	1-3 miles	3-5 miles	3-5 miles	1-3 miles

Table 9. A Comparison Between WiMAX Standards (After: [27]).

c. WiMAX Interoperability

The means to IEEE 802.16 interoperability is the IEEE 802.2 Logical Link Control (LLC) Service Access Point (SAP), which is common to all IEEE 802 networks. It accepts and transmits datagrams and frames then it passes them back through the protocol stack to a router. The router relays them to the next network segment [1].

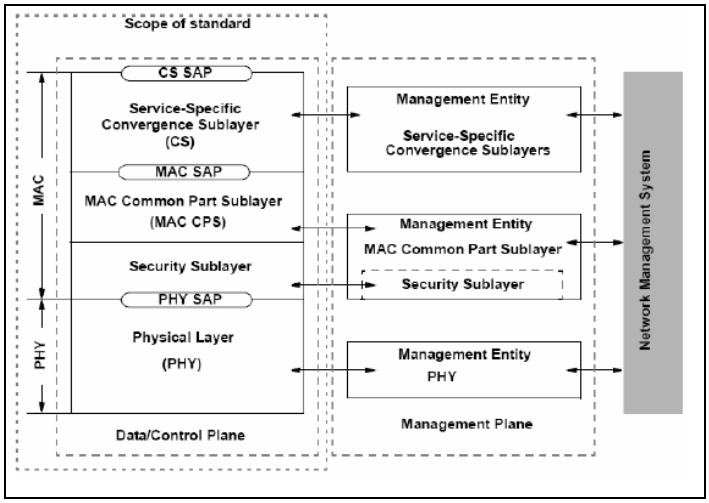

Figure 17. Protocol Structure (From: [33]).

The Physical (PHY) layer is frequency-dependant, which means that only this layer is to be changed if a different medium is used. Generally, WiMAX uses Orthogonal Frequency Division Multiplexing (OFDM) technology at the PHY layer [1].

Figure 18 depicts that the Physical Medium Independent (PMI) sub-layer (top half of layer 1) and the MAC (layer 2) are entirely frequency-independent (layer modularity).

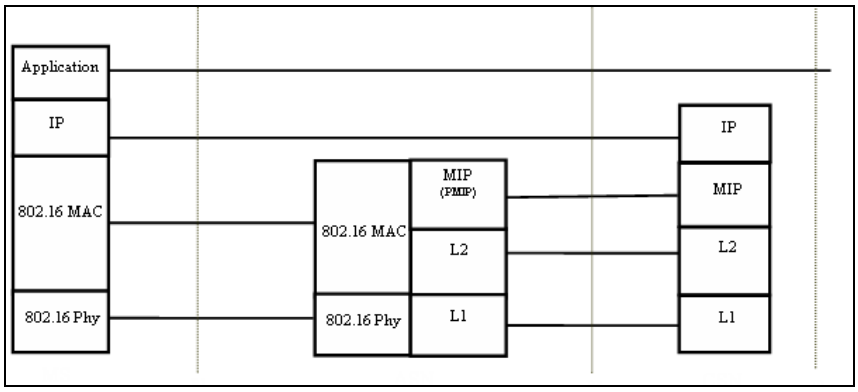

Figure 18. WiMAX MAC Layer (From: [33]).

Similar to all IEEE 802 networks, WiMAX is routable. Within the network segment, WiMAX has a stable MAC. The scheduling algorithm in WiMAX provides three major benefits: stability under overload, bandwidth efficiency, and ability to control QoS.

OFDM has some advantages over other technologies, lower power consumption, minimum bandwidth usage, and efficient bandwidth usage. OFDM provides better channel throughput because all of the underlying sub-carriers are orthogonal to one another. Table 10 compares the parameters regarding fixed WiMAX and Mobile WiMAX OFDM PHY layer [32].

Parameter	Fixed WiMAX OFDM-PHY	Mobile WiMAX Scalable OFDMA-PHY			
FFT size	256	128	**512**	1,024	2,048
Number of used data subcarriers	192	72	**360**	720	1,440
Number of pilot subcarriers	8	12	**60**	120	240
Number of null/guardband subcarriers	56	44	**92**	184	368
Cyclic prefix or guard time (Tg/Tb)	1/32, 1/16, **1/8**, 1/4				
Oversampling rate (Fs/BW)	Depends on bandwidth: 7/6 for 256 OFDM, 8/7 for multiples of 1.75MHz, and 28/25 for multiples of 1.25MHz, 1.5MHz, 2MHz, or 2.75MHz.				
Channel bandwidth (MHz)	3.5	1.25	**5**	10	20
Subcarrier frequency spacing (kHz)	15.625		**10.94**		
Useful symbol time (μs)	64		**91.4**		
Guard time assuming 12.5% (μs)	8		**11.4**		
OFDM symbol duration (μs)	72		**102.9**		
Number of OFDM symbols in 5 ms frame	69		**48.0**		

Table 10. OFDM Parameters Used in WiMAX (From: [32]).

d. WiMAX Security (Authenticity)

The WiMAX security is aimed at improving infrastructure security, and is particularly resistant to TOS attacks. It supports encryption, authentication and other security mechanisms. WiMAX is vulnerable to a replay attack in which an attacker maliciously resends valid frames that the attacker has intercepted in the middle of the forwarding (relaying) process. WiMAX increases the level of network security by using both terminal and subscriber authentication to stop a possible theft of service.

Encryption mixes data using a mathematical algorithm with a ciphertext output which will be transmitted using the wireless network. The eavesdropper will not be able to understand the ciphertext. WiMAX uses Advanced Encryption Standard (AES), the block cipher ratified as a standard by National Institute of Standards and Technology of the United States (NIST), for this process. AES input is a mixture of an encryption key and a counter with a bitstream output as shown in the Figure 19. The next step is to apply an exclusive OR operation on the bitstream and the data to produce the ciphertext. At the receiver, the reverse process will be applied (same encryption key must be used at both ends) [28].

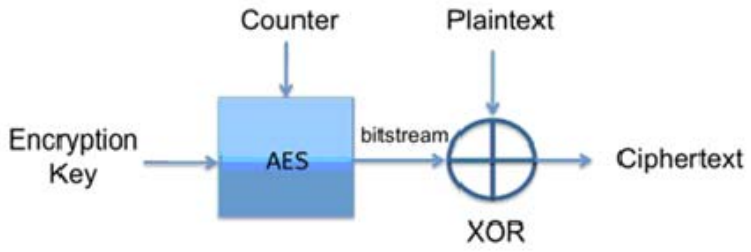

Figure 19. AES Encryption (From: [28]).

The IEEE 802.16e-2005 standard uses the Privacy and Key Management Protocol version 2 (PKMv2) to secure the key transfer between the Base Station (BS) and the Mobile Station (MS).

PKMv2 produces an Authorization Key (AK) which is utilized to derive the encryption key. PKMv2 also supports the use of Rivest-Shamir-Adlerman (RSA), which is an algorithm for public-key cryptography and it is the first algorithm known to be suitable for signing as well as encryption, exchange which requires a manufacturer-issued X.509 digital certificate or a Subscriber Identity Module (SIM) card [28].

Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which the key used to encrypt a message differs from the key used to decrypt it.

In case of X.509 (X.509 is an International Telecommunication Union (ITU) standard for a public key infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI)) digital certificate, it will contain the mobile station's Public-Key (PK) and its Media Access Control address (MAC address) (which is a quasi-unique identifier assigned to most network adapters or Network Interface Cards (NICs) by the manufacturer for identification) which will be validated by a certificate authority as shown in Figure 11 [20].

Figure 20. Public Key Infrastructure (From: [28]).

The IEEE 802.16-2005 supports the device and user authentication, privacy, and validation. It is able to dynamically refresh keys and detect replay attacks. 802.16-2004 only requires SS to be authenticated. 802.16-2005 security is better than 802.16-2004 as it requires both SS and BS to be authenticated [1].

e. IEEE 802.16 Quality of Service (QoS)

WiMAX supports high level of Quality of Service (QoS). The WiMAX QoS parameters could include traffic priority, burst rate, scheduling type, delay, jitter, Service Data Units (SDU) MAC signaling type and size [29].

WiMAX, by its MAC, implements bandwidth efficiency and trades off other QoS characteristics, which is almost always the correct tradeoff [1].

f. WiMAX Evaluation

An evaluation of WiMAX technology for emergency communications could be derived. WiMAX is Hastily Formed Network (HFN) enabled, mobile and usage flexibility is in the core of its attributes.

(1) Performance. WiMAX has a reputation as the best alternate solution for wireline-equivalent broadband service. 70 Mbps speeds at 50 Km range are often mentioned as the actual performance for users, while this is the total shared bandwidth capacity available to multiple users on 2X20 MHz frequency spectrum (2X20 MHz refers to the Frequency Division Duplex (FDD) mode). Actual per user data rate is

1-3 Mbps. The 50 Km usage is for LOS deployments while expected coverage is 1-3 Km in urban areas and 5-10 Km in rural areas [33].

(2) Low cost CPE availability. WiMAX CPE is still pre-standard and expensive. It will take years to get the economy of scale limit.

(3) Fixed-WiMAX vs. ADSL. Broadband in Jordan is experiencing breathtaking progress as offers for this service are getting cheaper and cheaper. In light of the wired presence, WiMAX has to be very competitive in terms of price and services offered. However, in rural areas with poor wireline infrastructure, WiMAX is definitely more economic and has benefits over ADSL. When comparing the services offered by the two technologies, wired broadband still better than WiMAX. Wireline can offer higher bandwidth which supports voice, broadband, TV and Video-on-Demand to customers [2].

D. POWER TECHNOLOGIES FOR COMMUNICATIONS

Communications technologies support systems are vital for the continuity of the service during emergencies. Backup power systems should be ready to take over when the electricity grid is out of order. It is important to remember that without power, all of the advanced technology will not help. Special consideration for power distribution is vital as follows [1]:

1. Storing and Retrieving the Power

Batteries are the classical solution for storing and restoring power. It limitations such as: large size, high weight, and hazardous materials make it logical to think about other options such as capacitors.

2. Estimate the Power Consumption

An estimate for the power draw results in an estimate for the power sources needed on site to provide for 24/7 operation.

3. Generators and Fuel Cells

As generators require refueling; the logistics of fuel in a disaster emergency can be a burden. Wind or crank power may be options along with Photovoltaic cells (PV).

a. Photovoltaic Cells (PV)

First developed in the mid-1950s, PV power cells (also named Solar Cells) convert light photons into electricity, using panels made of thin films of semiconductors materials such as Silicon and Germanium. These systems are friendly for the environment, have low-noise, have no fuel consumption, are maintenance-free, and have no running cost. Figure 21 shows a basic PV in operation [10].

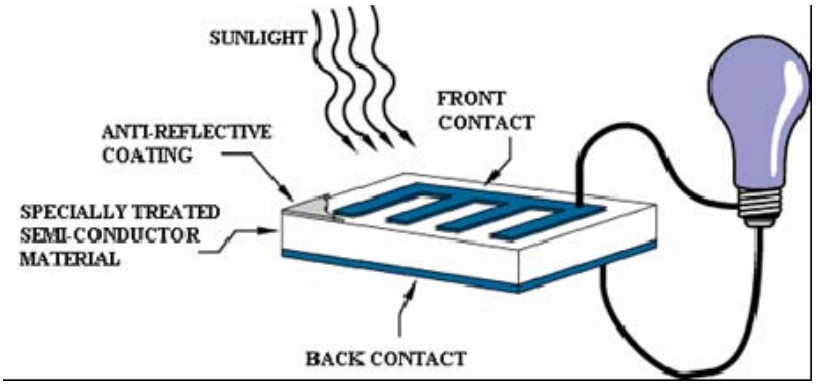

Figure 21. Operation of a Photovoltaic Cell (From: [10]).

PV has the potential to be used in emergency systems where the grid power is not available. PV works when there is adequate sunlight and should be coupled with storage devices (batteries). Power is needed at the fringe, as this is what makes the Photovoltaic solution attractive and it can be deployed with each subscriber station.

b. Mobile Generators

Generators are centralized power systems which are often not suitable for highly distributed applications. Mobile generators are a potential solution but have a logistics problem of re-fueling [11].

c. Fuel Cells

Fuel cell technology is rapidly emerging as an alternative to incumbent battery backup power in communications infrastructures. Fuel Cells also allow distribution (without the dependence on sunlight), there are new fuel cells emerging that are sized for laptops, cell phones, and other portable devices [11].

E. SUMMARY

In this chapter, different communication technologies was elaborated upon, evaluated and compared. WiMAX and WiFi technologies have the potential to be employed in the disaster recovery arena. TETRA and iDEN are already implemented in Jordan, which is saturated with three GSM operators.

VI. JORDAN'S INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ENVIRONMENT

By the year 2000, Jordan became a full member of the World Trade Organization (WTO). This membership has led to being fully liberalized in the ICT sector in Jordan by the end of year 2004. To eliminate monopoly, the ICT sector has been privatized and opened for competition which alleviated the level of services issues to the public [53].

Jordan is considered one of the pioneers in the region in the field of ICT. The ICT infrastructure and technical human resources are growing fast. A survey of the current ICT infrastructure available in Jordan is necessary to craft a suitable Emergency Communications Interoperability Plan (JECIP) for Jordan.

Jordan's ICT infrastructure is based on Circuit-Switching technologies along with ongoing Packet-Switching projects in Jordan. Packet-Switching will be the core technology of Jordan's future ICT infrastructure due its many benefits in comparison with Circuit-Switching.

Analysis should take into consideration the assets of both public and private sectors. Following is a discussion of important aspects of the ICT environment in Jordan.

A. AUTHORITY

1. The Communications Licensing Authority

The Communications Industry within Jordan is regulated by the Telecommunications Regulatory Commission (TRC). The TRC grants licenses to communication operators, supervises the licenses, conducts spectrum management, and issues type approval. The TRC has the authority of approval for telephones, facsimile machines, modems, PABXs, and all other types of communication services.

2. The Disaster Management Authority

The Higher Committee for Emergency and Crisis Management is a country wide committee established to deal with disaster related incidents in Jordan. This committee is comprised of all bodies and organizations which have the potential and responsibilities for public services. In the case of emergencies such as bad weather or an avian flu

pandemic event, the committee gathers in an operation center to arrange for response and aid to the affected areas. Communication is a key component in the response plan as it is vital for different government sectors to perform their tasks efficiently and with mutual cooperation and coordination.

Jordan has a local committee for emergency response planning and crisis management for each major component of the country's government. Jordan's Armed Forces (JAF) is a pioneer in this regard; the committee for emergency and crises management is a well-established body and has access to all communications assets available. Other components of government have their own committees and react to emergencies with respect to their tasks. The Directorate of Public Security (DPS) (Police) has a committee which controls its communications network and has nation-wide coverage responsibility. The General Civic Defense (GCD) (Fire Fighters) organization also has its own committee and reacts to minor emergencies on a daily basis

The Ministry of Information and Communication Technology (MoICT), the Ministry of Interior (MoI), and several other agencies have cooperated in the process of drafting a national emergency plan for the Jordan's communication sector. The plan is designed to help maintain the communication infrastructure in emergency situations.

When ready (expected by 2010), Jordan's National Crisis Management Center (NCMC) will be the sole authority which will handle the planning and implementation of Jordan's emergency communication plan. It will take over that authority from MoICT and other agencies in this regard.

The under-construction NCMC is proposed to be the nodal point at the national level for disaster mitigation and response which is based upon connecting all parties in response to emergencies.

The NCMC will consist of several subcommittees such as The National Council for Disaster Management which set the policies underlying the national disaster management plan. Another subcommittee is the Technical Advisory Group (TAG) which will assist in the preparation of the national disaster management plan in terms of

information technology and communication. The Vigilance Groups (VG) subcommittee will be spread around the country to monitor disaster signals and will be the first line of disaster detection.

The local government agencies in the area of the crisis will deal with the emergency and start reporting to the NCMC through the Vigilance Groups (VG) which will evaluate and decide the size of intervention required for the government and other agencies.

3. The Emergency Communications Plans

Communications systems should provide the means by which resources can be accessed, mobilized, managed, and coordinated in both normal and adverse situations. Communications systems must therefore employ sufficient communications paths and operational capabilities among all participants to facilitate the functional communications concepts.

The following military and security agencies have their own emergency communications plans: Jordan Armed Forces (JAF), Directorate of Public Security (DPS), Directorate of Civil Defense (DCD), Headquarter of Gendarmerie Forces (GF), and General Intelligence Directorate (GID).

All of the above agencies have a VHF or UHF dispatching Push-To-Talk (PTT) system but these systems will be replaced by a TETRA system shortly, so there is no need to make any modifications to the current dispatching systems.

Jordan Armed Forces and Police participate in UN Peace-keeping missions all over the world. These missions require versatile types of communications systems, especially HF links and satellite phones (Thuraya & Inmarsat).

The following companies and agencies have their own emergency communications plans: Water Management Company, Electricity Generation & Distribution Company, Ministry of Information and Communication Technology (MoICT), Ministry of Health, and the Ministry of Public Works & Housing.

All of the above agencies have a VHF or UHF dispatch Push-To-Talk (PTT) systems. Modifications for the current dispatching systems are necessary to be able to talk to other agencies and to be connected to the main backbone.

Recommendations: NCMC (when active) should take over. Agencies with dispatching systems should be included in the future TETRA system.

4. Non-Governmental Organizations (NGO)

There are several NGOs in Jordan which contribute to disaster relief activities such as The Jordan Red Crescent (JRC), the International Federation of Red Cross and Red Crescent Societies (IFRC). These NGOs are engaged in mitigating natural disasters. The International Committee of the Red Cross (ICRC) focuses exclusively in mitigating man-made disasters.

B. JORDAN'S ICT INDICATORS

For a country of almost six million people, Jordan has 450,000 fixed telephone lines and 3 million cellular phones. The government agencies are connected by landline phones and fax. The backbone for this landline network is mainly microwave and fiber optics. Most of these agencies have cellular phones. The ambulances run by the DPS, the JAF and the GCD are equipped with VHF radios. PABX links all government hospitals in Amman.

The following infrastructure components are already active in Jordan: Optical fiber (military and civilian), WiMAX (Amman area), Landline (PBX) old circuit switching infrastructure), Cellular (GSM), and iDEN.

The telecom operators should ensure that their systems are resilient for different types of disasters ranging from mild snow, floods, and landslides to fire. Jordan is susceptible to terrorist attacks as well. The operators should have disaster-kits ready to be moved to a disaster site and have a disaster recovery plans standing by to repair damaged portions of their network.

1. The Fixed Line Sector

Jordan has been emphasizing the enhancement of their human capital, the macroeconomic conditions and the business and government environment. The momentum behind this enhancement process includes public private partnerships with international and regional companies. This process has been formed to undertake many initiatives to achieve countrywide development [53].

The current fixed line infrastructure in Jordan is very reliable and robust. Enhancements for the Infrastructure such as the establishment of National Broadband Network (NBN) will give the network better resilience and reliability. The Internet and mobile usage is moving toward better coverage and connectivity.

There are still bottlenecks for the communication sector in Jordan such as the regulatory and affordability issues that impede higher usage of these technologies.

Number of Subscribers:	**2000**	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**
Fixed Phone	620000	660000	674000	623000	638000	628000	614000
Mobile & Trunking	389000	866000	1200000	1325000	1624000	3138000	4343000
Paging	12000	4400	4600	2300	2100	2200	2100
Internet	32000	66000	62000	92000	111000	197000	206000
Population	4820000	4940000	5070000	5200000	5350000	5489100	5600000
Main Telephone lines per 100 inhabitants	12.86	13.36	13.30	11.97	11.92	11.4	11
% of residential main lines	78	77	78	79	78.9	77	72
% households with a telephone	60	63	60	55	52	64	59

Table 11. Telecom Main Indicators in Jordan (After: [12]).

The above table gives a metric for penetration without measuring the availability in general or at a component level. Redundant connectivity and the presence of backup power and the ability to perform fault detection need to be addressed for a true picture.

2. Mobile Market in Jordan

In the market of mobile communications, many companies provide coverage and services in this booming business. Jordan enjoys high cellular technology users' count. The ratio of cell subscribers to the population is almost 75%. That rate may be reduced to 50% when omitting users having more than one cell lines.

In 1995, Fastlink (now Zain) was the first GSM mobile network that started its services. By the year 2004 four operators were to compete in the market (3 GSM and 1 iDEN operator). Table 12 depicts the percentage of market share between those operators.

Company	Established	Technology	Subscribers (end of 2006)	percentage
Zain	1995	GSM 900	1,961,000	48%
Orange	2000	GSM 900	1,405,500	30%
Umniah	2005	GSM 1800	700,000	10%
Xpress	2004	iDEN	65,000	2%
Total			4,131,500	100%

Table 12. Percentage of Mobile Operators in Jordan's Communication Market (After: 46]).

TRC published a request for bid for the 3G as a new service in Jordan. If no current operator succeeds in acquiring the 3G license, a fifth new operator will start its services in Jordan. The following are the mobile operators in Jordan [46]:

a. Zain Company

The following figure depicts the map coverage for Zain GSM operator.

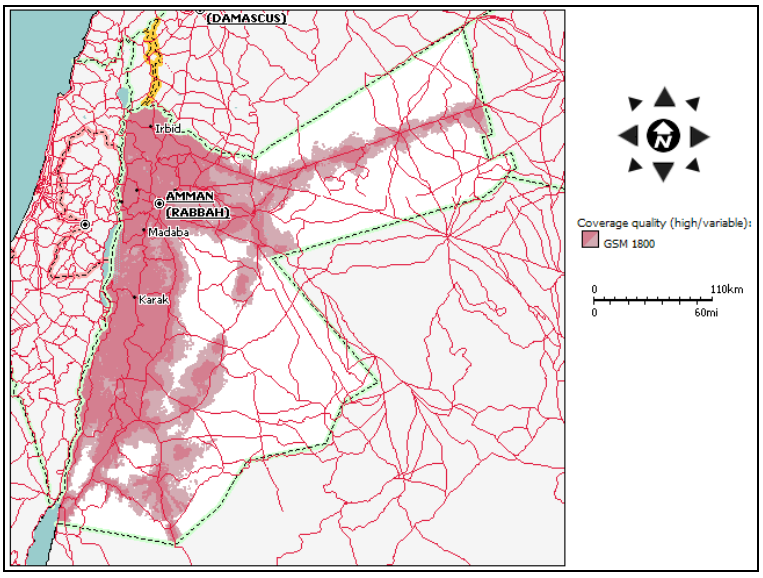

Figure 22. Zain Coverage Map in Jordan (From: [46]).

Recently, a new era has been started in terms of roaming - led by Zain. Zain is an active operator in 22 countries in the Middle East and Africa. A user could call any other user in these 22 countries as if they are in one network without the need of roaming services. This will make it easier and cheaper for NGOs and other aid agencies to talk in different countries.

b. Orange Company

The following figure depicts the map coverage for Orange GSM operator. It seems that Orange has the best of these converges especially in southern and eastern areas.

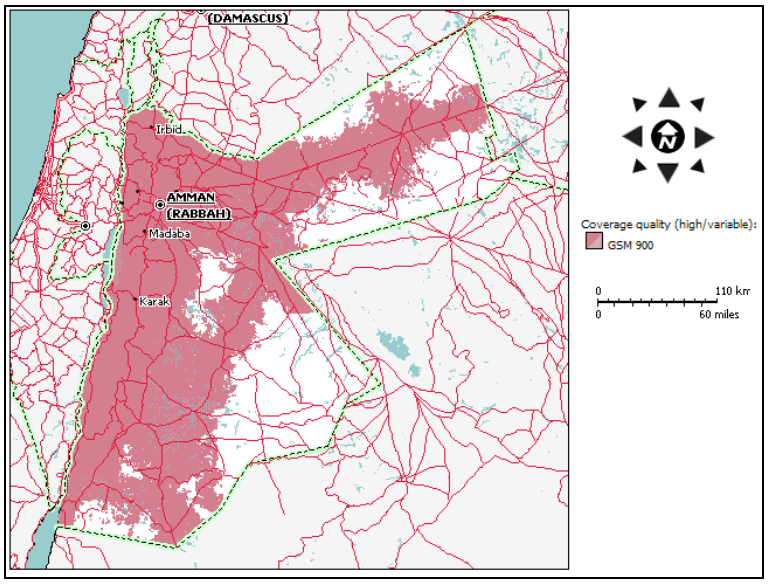

Figure 23. Orange Coverage Map in Jordan (From: [46]).

c. Umniah Company

The following figure depicts the map coverage for Umniah GSM operator.

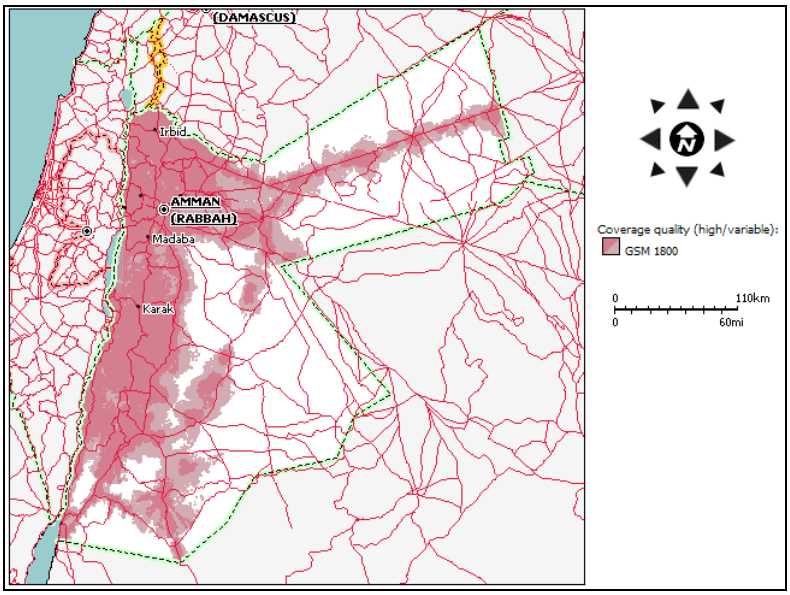

Figure 24. Umniah Coverage Map in Jordan (From: [46]).

d. Xpress Company

Jordan's experience with the iDEN system is not very successful as it has only 2% of Jordan's commercial mobile market (not meant for emergency communications services). The iDEN technology is a Motorola proprietary system which makes it an expensive service. The terminals are also expensive and no third party produces or maintains iDEN products which will hinder the spread of the service.

An agreement should be negotiated between those operators to enable access for other users for all networks in case of emergency. Another solution for the coverage issues is to have mobile base stations which will be deployed in the area of the emergency.

3. The Internet Sector

Table 13 shows the population statistics in Jordan compared to the growth of the Internet. According to the International Telecommunication Union's (ITU's) table, the Internet users in Jordan are growing dramatically. Expectations for Internet usage are to grow to 50% by the year 2010.

YEAR	Users	Population	% Pop.	Usage Source
2000	127,300	5,282,558	2.4 %	ITU
2002	457,000	5,282,558	8.7 %	ITU
2005	600,000	5,282,558	11.4 %	ITU
2007	796,900	5,375,307	14.8 %	ITU

Table 13. Internet Growth and Population Statistics (From: [12]).

To measure the level of ICT in any country, the e-readiness concept was developed. All of the factors of communications and Internet infrastructure which add up to a broad concept may be called e-readiness. The definition of e-readiness is the level of preparation of a country to participate and benefit from Information and Communication Technology (ICT) developments. In other words, the usage level of ICT directly relates to conducting standard expected functions of the government and citizens [41].

Table 14 depicts the rank of Jordan with respect to other countries in the world. Categories used to test e-readiness include connectivity and infrastructure. Jordan enjoys a relatively good position on the scale (medium), which makes it better than many neighboring countries.

Country	Connectivity and Infrastructure	Human Capital	Macroeconomic Structure and Business Environment	Government	IT Industry and Innovation Capacity
USA	High	High	High	High	High
Singapore	High	High	High	High	High
Canada	High	High	High	High	High/medium
Ireland	High/medium	High	High	High/medium	High/medium
UAE	High/medium	Medium	Medium	High/medium	Medium/low
Turkey	Medium	Medium	Medium	Medium	Medium
India	Medium/low	Medium	Medium/low	Medium	High/medium
Mexico	Medium	Medium/low	Medium/low	High/medium	Medium/low
China	Medium	Medium/low	Medium	Medium	Medium/low
Jordan	Medium	Medium	Low	Medium/low	Medium
Egypt	Medium	Medium/low	Low	Medium	Low
Kuwait	Medium	Medium/low	Medium/low	Low	Low
Lebanon	Low	Medium	Low	Low	Low
Morocco	Medium/low	Medium/low	Low	Medium/low	Low

Table 14. The rank of Jordan with Respect to Communication Categories (After: [41]).

4. Applications

a. Telemedicine

A telemedicine network started in Jordan's hospitals several years ago. Patients X-rays and records are shared through the network. Some National Hospitals have telemedicine networks with hospitals in the U.S.

b. Alert Systems

Jordan has very limited access to the sea, Aqaba port, so a city-wide alarm system is not necessary as the Tsunami threat is very low. Other parts of the country need a multipurpose alarm system for public warning from disasters.

5. Satellite Phones

In the case of Jordan, this technology is not well utilized as it is still relatively expensive. If necessary, the Thuraya and Iridium networks offer satellite phone coverage in the region and other parts of the world which could be used in emergencies inside and outside of Jordan.

6. Wireless Technology in Jordan

a. WiFi

In case of Jordan, this technology is evolving and many Internet Service Providers (ISPs) are implementing hot spot all over the country. Zain and other telecom operators started an initiative to make this service available on certain university campuses in Jordan. Cafes and Malls started to offer this service as a complementary offering to their other services [52].

b. WiMAX

In 2006, Umniah and Atco Companies started the Fixed Broadband Wireless Access (FBWA), in other words, WiMAX.

Umniah, the Jordanian mobile provider and a subsidiary of Batelco Bahrain has launched WiMAX services under its new trademark, UMAX. Wi-tribe is the second WiMAX ISP operator. Wi-tribe Jordan is a subsidiary of the regional telecommunications company Wi-tribe limited, which is a joint venture between Qatar Telecom (Qtel) Q.S.C and A.A. Turki Corporation for Trading and Contracting (ATCO) of Saudi Arabia [2].

WiMAX coverage is still limited to Amman, the capital, but future expansion is inevitable.

C. ICT INITIATIVES IN JORDAN

Jordan started a National Strategic Plan to reform the communications and Information and Communication Technology sectors. This strategy has several themes:

elimination of monopoly, withdrawal by Government in favor of a private sector led market environment, and, social and demand development through access to education and widened opportunity.

Still there are certain issues that should be clarified, the problem of dual standards in governments, as this non-monopoly strategic point should apply to all projects and initiatives in progress in Jordan (even if owned by the government).

New communications technologies are being introduced to the public which made the communication infrastructure more advanced and robust. In parallel, the commercial/public Internet services have been enhanced. Intranet pilot projects such as the Jordanian E-government, E-army, E-health, and E-education are being implemented.

All of these projects from different public and private sector entities make Jordan's communication environment well defined and relatively sophisticated. This advanced infrastructure will reflect on the country's readiness for disasters and emergencies.

1. Connecting Jordanians Initiative (CJI) Overview

CJI was introduced by MoICT to improve the lives of Jordanian citizens and furnish an infrastructure for the telecommunications sector to bloom. Part of this initiative was to establish a broadband learning public access network which links schools, colleges, universities, and telecenters by 2005 [53].

2. National Broadband Network (NBN)

For the success of CJI, the need for a broadband fiber network is essential. The scope of the project is: University Broadband Network (8 public universities and 9 sites), School Broadband Network (3300 public schools, 100 knowledge stations, 17 public community colleges, and 12 learning resources centers). NBN is very convenient as a backbone for communication safe spots in case of emergencies, with an understanding that modifications will be added to the network so that it will meet future emergency services needs. Jordan should focus on improving availability in terms of location and redundancy as it will be cheaper to implement than creating new infrastructure [53].

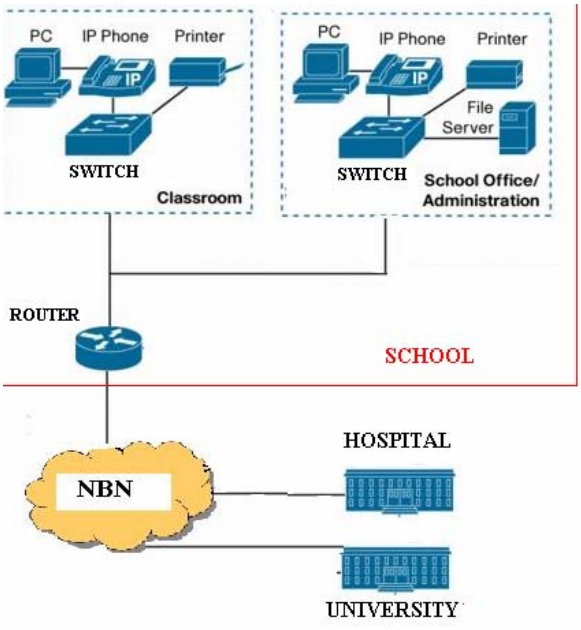

Figure 25. NBN School LAN.

Although both are supported by the same government, NBN is not integrated with the emergency services network. Schools are often emergency services staging sites and are often used as refugee centers. This is the reason why extending the Internet using WiMAX would be an economic and feasible solution.

3. E-government Program

The e-government program mission is to support transformation to enhance the government efficiency using information technology and communication tools. Business Process Re-engineering (BPR), Human Performances Development (HPD), and deploying the best practices with latest technologies are the main aspects of program implementation [53].

4. TETRA

In 2006, The Jordanian Defense Ministry awarded Thales Company a contract to provide a nationwide TETRA network. The network will include 70 base stations and provide secure communications services for 20,000 users. The network is based on a distributed architecture qualified under real operating conditions and standard IP routers.

TETRA is the ideal for government-to-government and inter-agency communications. Other parts of the infrastructure should be tied to this network via gateways and proxies which will offer connectivity for citizens in both directions.

The network can be shared by Jordan's Armed Forces (JAF) both (Army, Air Force, and Special Forces) and will be extended later to include the Directorate of Public Security (DPS) (Police), General Civic Defense (GCD) (Fire Fighters) and other organizations [25].

The Jordanian government selected the Thales DIGICOM25 solution to deliver its entire nationwide TETRA capability. DIGICOM25, the full TETRA-over-IP communications network, is part of a range of solutions using Internet Protocol (IP) to communicate over the infrastructure network. It provides TETRA-standard digital communications service which includes voice, data, and imagery. DIGICOM25 allows the flexibility of IP routing and distributed configurations which provides high level of reliability. It provides interoperability with TETRA terminals and other access networks [37].

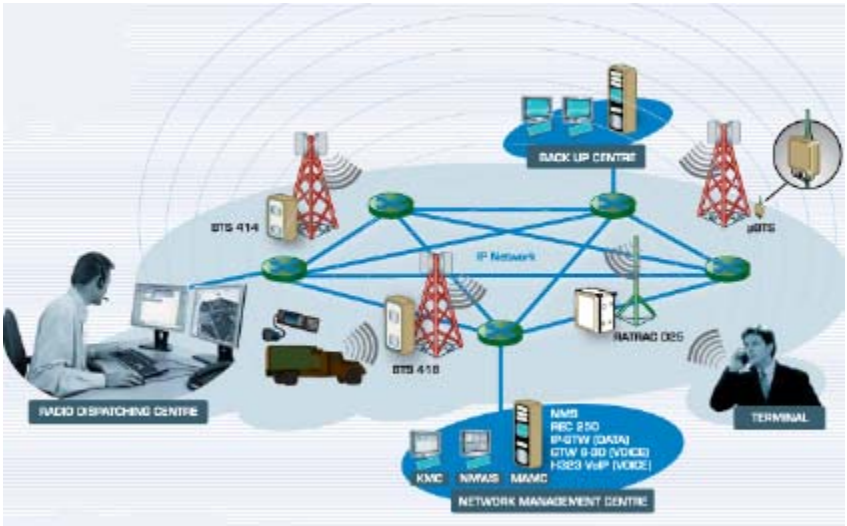

Figure 26. DIGICOM25 Network Architecture (From: [37]).

DIGICOM25 is developed for both civil and military markets, these innovative products make it possible to replace proprietary switches with standard IP routers, thereby offering significant savings in terms of both initial outlay and operating costs.

Dispatching and fleet monitoring functions use Commercial off the Shelf (COTS) equipment and is managed on standard PCs running Windows software, making the system even more economical. Native security including Class 1 to Class 3 encryption and dynamic key management for authentication make network sharing possible. The following table depicts the main attributes of the DIGICOM25 system. As mentioned above, DIGICOM25, the full TETRA-over-IP communications network, TETRA network to be implemented in Jordan is based on a routed technology [37].

Attribute	**Description**
Services	Half and Full Duplex calls Group calls PSTN/PABX calls (individual and group) Emergency calls , Priority calls
Security	Network class 1,2,3 End-to-End encryption Key management center Mutual authentication
Network Management	Statistics tools Alarm management (SNMP) QoS support mechanisms
System interface and gateways	Dispatcher PABX/PSTN ,H.323 VoIP, SDS, DATA gateways Automatic Vehicle Locator GSM networks

Table 15. Thales DIGICOM25 TETRA Solution (After: [37]).

The users, Jordan's Armed Forces (JAF) are not enthusiastic about using this feature due to security concerns. These concerns include a lack of security of the Internet such as viruses and breaches. The users would like to create a closed network. This will make it hard to acquire high availability of the network. Also, this will be a fundamental incompatibility [1]. The use of this network for public safety is suggested in this thesis which needs an administrative decision and technical alteration.

The technology is still under construction in Jordan so no current evaluation is available. The attributes and services on paper are promising and if used well will be a good solution especially in case of emergencies.

D. INFORMATION GATHERING DISSEMINATION IN EMERGENCY

Before a crisis strikes the country, a campaign should be started to create a public awareness of the roles of different agencies and governmental divisions in case of emergency. Citizens should also understand their roles and responsibilities and what they should prepare in their homes and work places to be ready for any emergency. Basic survival kits, special radio receivers, extra cell phone batteries, and plugs to charge from cars are examples of these precautions.

There are several communication technologies to be used in case of emergency. An assumption that an incident does destroy the communication infrastructure in the area will lead to the following procedures to be started:

1. Gathering Information

The Ministry of Interior (MoI) provides weather and emergency status to radio and TV stations, for remote sites, word of mouth is still a prevalent form of communication. SMS and E-mails may be the new methods of information dissemination to citizens in the country.

Call centers will be arranged to receive missing-persons update and get feedback information to improve situational awareness in both sides.

2. Dissemination

a. TV and Radio Broadcast

An update for the current status of the incident area will be broadcast via TV and radio. An example for an incident is the spread of an epidemic, the information and countermeasures needed by citizens disseminated via TV (VHF,UHF) stations, radio (AM, FM) stations, and satellite channels. Public or private owned media should be at

NCMC disposal for that purpose. Discrete, short, clear, and authenticated messages should be broadcasted to include communicating with disabled persons for access to the information.

b. Other Broadcast Media

New broadcast media will be used such as podcast, SMS, and Internet sites. SMS will be arranged through service providers to be sent to all cell phones users.

The information flow among the various agencies involved in disaster relief is currently vague and needs more coordination and planning due to multiple agencies and ministries being involved in the process.

There are four communications needs; each one needs an appropriate amount of attention as elaborated in Table 16 [1]:

Communications Need	**Available Technologies**
Government- Government	TETRA, VHF, and UHF dispatch networks along with landline phones.
Citizen-Government	Call centers and Landline 800 numbers.
Citizen-Citizen	GSM and iDEN Networks along with Landline Phones.
Government/Military-NGO Community	Satellite phones in addition to the above means of communications.

Table 16. The Four Communications Needs in Jordan (After: [1]).

E. INTEROPERABILITY IN JORDAN

Interoperability in Jordan is still a new concept. There is no specific guidance for new equipment procurements. The core of interoperability (nation-wide) is at both the agency and agency-to-agency levels. Jordan's main problematic interoperability issue is within the procurement cycle control. Each agency or ministry has its own policies and technical requirements [1].

Telecom operators and ISPs in Jordan should adhere to the TRC's interoperability guidelines as part of their license requirements. For military and security agencies, the new project TETRA network is under construction. TETRA will connect all of these agencies together with one network. Adding a group to this network for users based on their role in emergency response would enable all First Responders Community (FRC) members to talk to each other easily in case of emergency.

Frequencies available to user agencies are described with associated special assignment limitations by TRC. Some frequencies are shared with more than one agency. The national directory for the active frequencies in Jordan is maintained by TRC as it is the sole authority for administering the frequency spectrum.

Most public safety communications radios (portable, mobile, base station and repeaters) broadcast frequencies between 30 MHz and 900 MHz which are dedicated to public service use. Cell phones and other systems, such as global positioning receivers, call boxes, electronic signs, irrigation systems, and mobile command units, that transmit information from remote locations, transmit in the microwave band between 1 GHz and 20 GHz. There are three primary reasons why agencies cannot talk to each other [12]:

First, there are four distinctive frequency bands (Low VHF, High VHF, UHF, 800 MHz Band) that are used primarily by the First Responders Community (FRC).

The second primary reason agencies cannot talk to each others is compatibility, even when using radio systems in the same frequency range, some radio vendors' products are not compatible. A bridging device, or gateway, is needed to connect disparate radio systems that are operating in the same frequency range.

F. CHAPTER SUMMARY

The main goal of this chapter was to evaluate and analyze Jordan's ICT infrastructure and environment. From the above analysis for Jordanian communication environment, it seems that Jordan has two divergent business models: Government-owned Internet infrastructure and the private sector-owned infrastructure. As mentioned earlier, WTO rules are against public-owned ISPs.

The solution for this issue is to encourage or facilitate creation of a private company which will be open for investment and will manage and exploit the infrastructure on a competitive basis and may be used by citizens and private companies. This would help to build an infrastructure with high availability and endurance against emergencies.

Although the dominant trend for the business model in Jordan is toward a private sector-owned infrastructure, a lot of work remains to be done to achieve this. GSM networks are very suitable to be used as an emergency backbone due to its coverage and availability.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. A PROPOSED JORDAN'S EMERGENCY COMMUNICATIONS INTEROPERABILITY PLAN (JECIP)

Based on the technological aspects of emergency communications, Jordan's communications environment, the requirements analysis of emergency communications plan, and lessons learned from the U.S. experiences with recent disasters discussed in earlier chapters a proposed Jordan Emergency Communications Interoperability Plan (JECIP) is introduced in this chapter.

The aim of this proposed JECIP is to improve the response readiness and efficiency of components involved in emergency. Parts of this plan are already in practice but the added value relies on the integration of plan components.

Generally, JECIP includes features such as redundancy for transmission routes, spares for vital equipment, backup subscriber management centre, emergency hot-lines, paging systems to spread disaster warnings, and rapid upgrading of base stations after a disaster. Guidelines for improvements of the plan are introduced. These guidelines are expected to be expanded by others in future work to draft a better JECIP for Jordan.

The core of JECIP is based upon the IP infrastructure. All other available infrastructure component and ICT systems are connected to the core through gateways. Various communications technologies and equipment types are discussed with a focus on performance parameters to evaluate communications equipment. Usually there are three qualifiers for equipment selection: economic, technological, and political.

A. JECIP OBJECTIVES AND SCOPE

1. Objectives

The main objective of JECIP is to make sure that the current communications infrastructure will be allow responders to talk to each other and assure that future equipment procurement will be according to specific interoperability and modularity standardization policies.

2. Scope

The scope of this plan is the ICT network infrastructure of Jordan. Interoperability is vital, as in cases of emergency; aid from outside Jordan is inevitable. Proper equipment and personnel training is important so the concerned agencies will use the same language and terminologies when working together in a Humanitarian Assistance/Disaster Relief (HA/DR) or Stability & Reconstruction (S&R) environment.

3. The Threat

The threat facing Jordan is similar to many countries, there are two types of disasters that may affect Jordan, natural and man-made. Fortunately, there have been no serious disasters to hit Jordan in the past 20 years. Most of those disasters were mild snow storms, low profile earthquakes, and small spread epidemics. But countries should plan for the worst and pray for the best. On the other hand, the main man-made disaster faced by Jordan is the bomb blast in Amman that occurred at 9 November 2005 (aka 9/11 of Jordan).

4. Plan Revision Procedure

A major goal in the development and distribution of JECIP has been to establish an effective revision procedure to ensure that all necessary information and requirements regarding emergency communications are promptly made available to all pertinent agencies.

B. JECIP AUTHORITY

TRC and NCMC should create an agency which will have the sole authority in drafting the interoperability guidelines for modular emergency infrastructure in Jordan. The proposed agency may be named Office of Communications Interoperability in Jordan (OCIJ). OCIJ (or whatever the new agency ends up being named) should create ICT equipment procurement strategies for better life cycle maintainability and make sure that the equipment will be interoperable and will be able to talk back to legacy systems. OCIJ includes a Joint Interoperability Test Center (JITC) to create an interoperability testing mechanism and assure vendor eligibility with respect to this testing process.

As part of the licensing regime handled by TRC, OCIJ will require that ICT systems providers follow certain guidelines relevant to the resilience of Jordan's ICT infrastructure. When TRC is to issue a license to a communications operator, OCIJ should have the authority to ratify the license. There are three emergency communication-related conditions that should be considered. First; the operator should be able to provide public emergency call service to emergency organizations for the purpose of an emergency, second is the need to provide plans for the provision and rapid restoration of communication services during public emergencies, and third is to provide emergency organizations with priority fault repair service fast [12].

C. JECIP APPROACH [1]

The proposed JECIP should leverage the existing Internet infrastructure and add the necessary high availability features to keep this fixed Internet component operating in all stressed situations. It is necessary to study these components with respect to interoperability and build one homogeneous network based on Packet-Switching technology and to connect Circuit-Switching components using gateways to the backbone.

The proposed infrastructure should have the ability to connect government to citizens and government to government. It also should have scalability for future expansion.

1. Packet-Switching vs. Circuit-Switching Technology

It is necessary to start building the infrastructure based on Packet-Switching technology for its scalability and flexibility. Economical factors play a part as roll-out costs are high in areas where Circuit-Switching technology is already installed. Those areas should be connected through gateways to the backbone.

2. Packet-Switching vs. Agency-owned Dispatching Systems

While agency-owned dispatching systems meet government to government communications needs, the Internet has the ability to meet all three of the communications needs in Jordan (citizen-citizen, citizen-government, and government-government).

This is the reason why the backbone for the proposed JECIP should be based on Internet technologies.

D. ICT SYSTEMS ENGINEERING STRATEGY

1. The Backbone

In this proposed JECIP plan, ICT infrastructure will be comprised of the IP network as a backbone. Being a routable network, other infrastructure components in Jordan will be connected to this backbone through gateways.

Figure 27 depicts the FRC network in Jordan. GSM, TETRA, VHF, UHF, NBN are connected though gateways to the IP network. Urban and remote areas are connected using WiMAX and WiFi fringes.

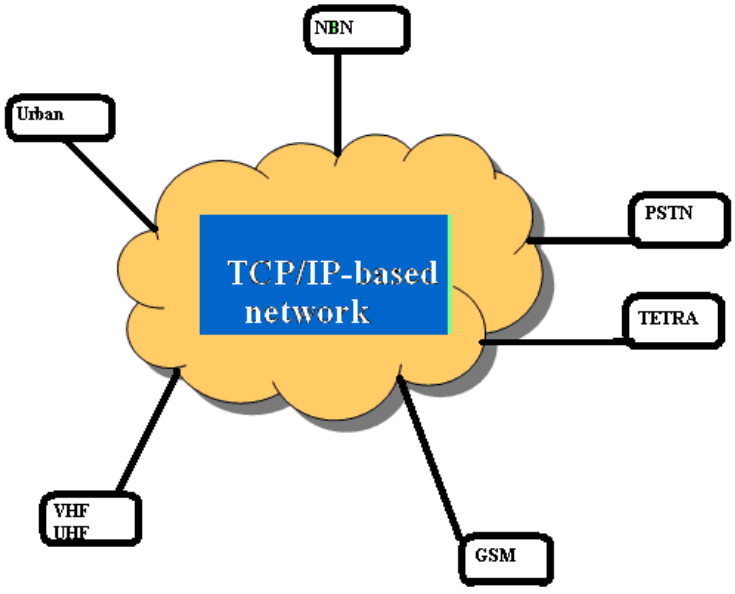

Figure 27. ICT Infrastructure Network in Jordan.

Figure 28 shows the communications network for Jordan's FRC members and UN troops outside of Jordan. The Thuraya satellite phones are used to connect to the IP network through a gateway.

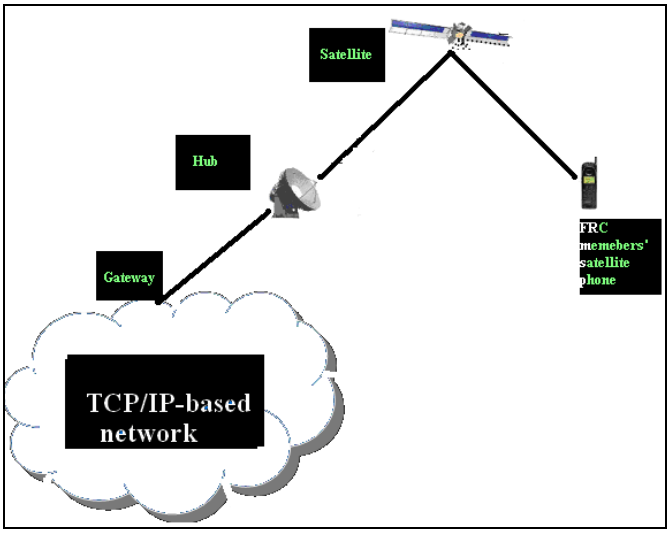

Figure 28. The Communications Network for Jordan's FRC Members and UN Troops When Outside of Jordan.

In the ICT context, NGOs operating in Jordan and surrounding countries (especially Iraq) need to be connected to the ICT infrastructure. International access to the outside world should take into consideration the load of traffic on the network during emergencies.

Figure 29 shows the communications network for NGOs when working in Jordan. Connecting to the FCR network in Jordan may be via Gateways or simply by adding a group for them with TETRA terminals.

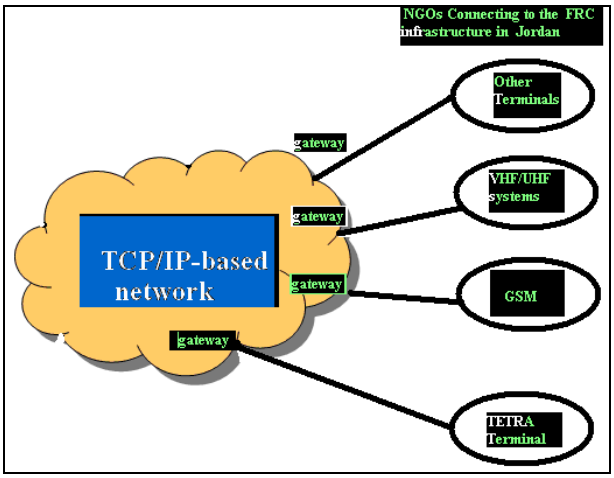

Figure 29. NGOs Connecting to the FRC ICT Infrastructure in Jordan.

Figure 30 shows the NBN network in Jordan which connects schools, Universities, and medical facilities (E-health project). These locations should be prepared to be shelters for citizens and FRC members in case of emergencies.

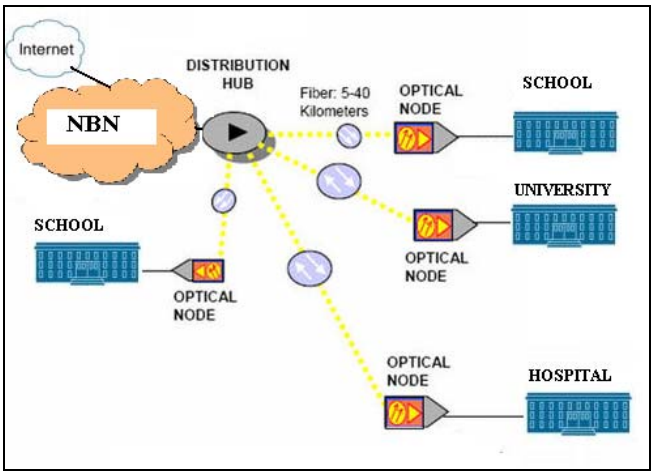

Figure 30. NBN Infrastructure.

2. Redundancy

The concept of back-up communications is, in general, the provision of sufficient equipment and procedures to enable an overall improvement in system reliability over time.

With regard to emergency communications specifically, the concept of back-up communications as applied to base stations or other fixed radio equipment is to enable primary dispatch communications to continue despite outage of the primary dispatch radio base station and to enable tactical communications to continue despite outage of the tactical radio base station.

Redundancy is an important issue to connect different parts of the network firmly. It is easily provisioned with routable network technologies not found in circuit switch technologies. Wireless technologies such as WiMAX, WiFi, and satellite are strong patching tools in case of losing a trunk between important parts of the network. Figure 31 shows a typical patching network.

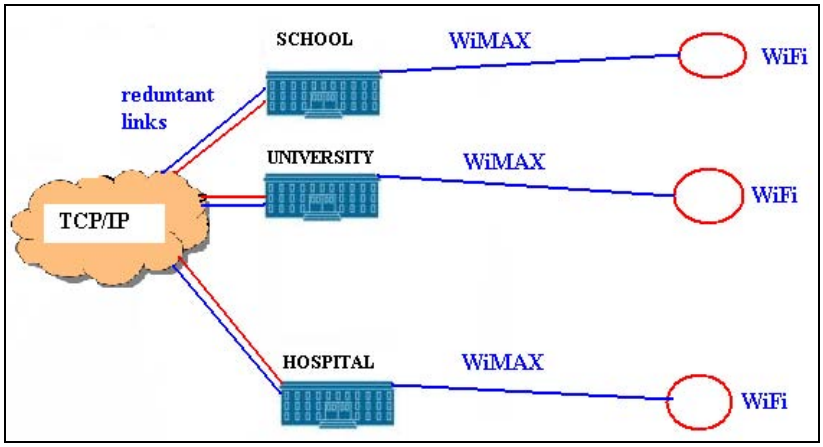

Figure 31. Patching and reach out.

In case the communications infrastructure fractures, NCMC will coordinate an assessment for the damage and try to patch the crack with one of the available assets. Technologies such as mobile GSM local cell with various backhaul connections such as WiMAX, satellite, or microwave will be available for the First Responders Community (FRC) in the field for the first three hours.

Evaluation and assessment teams will be on site as soon as possible to estimate the damage and decide how much resources are needed and to determine which the agency should provide these resources and coordinate these assignments with the pertinent authorities.

NCMC will work on the expansion of this network patch until the original infrastructure is back in service. Other technologies may be used for the same reason: satellite phones, WiMAX, WiFi. For the Internet, hotspots and Internet cafes will be available for the First Responder Community (FRC), official business, and the public (if possible). There will be limitations on streaming video or any big files, although some will have priority and should be accommodated – such as access to the missing-persons list for updates.

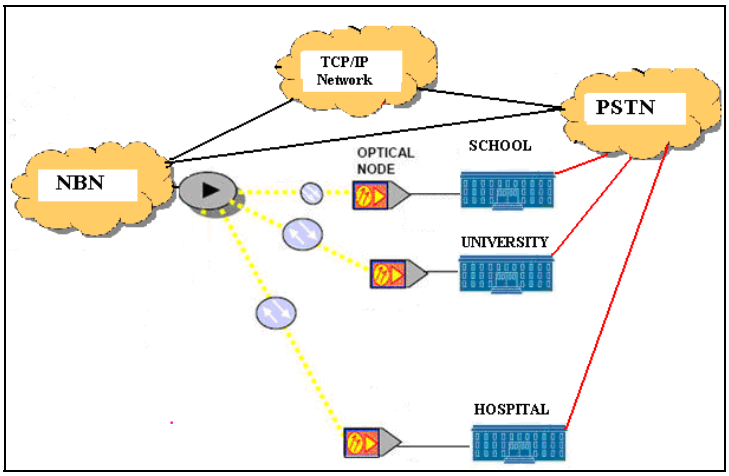

Figure 32. Redundancy Through Wireline.

Dual sites for these Points of Presence (POPs) should be created. All have at least two routes to other nodes. Backup power to critical nodes should be added. Fault monitoring equipment should be added also to reduce time between faults.

E. ICT FUNDING AND PROCUREMENT STRATEGY

1. Implement Indefinite Delivery, Indefinite Quantity (IDIQ) [1]

Consideration should be given to implement an Indefinite Delivery, Indefinite Quantity (IDIQ) procurement strategy via the proposed Office of Communications Interoperability in Jordan (OCIJ). Procurement committees and funds should have policies to help agencies which will cooperate in JECIP implementation.

The objective of these policies is to push agencies toward an interoperability solution in Jordan. The procurement process of products and services related to communications infrastructure will be probed by the OCIJ consultant teams so that they will make sure it is interoperable with the current systems.

The contracts for new communications equipments when conducted through an IDIQ procurement umbrella should be interoperable as they are bought from the same vendor.

The proposed OCIJ will help the technical specifications writers of different agencies to produce a specification that works with legacy systems already in service and interoperable with the systems to be procured in the future.

Communications systems require specific characteristics that will abide by the modularization model discussed in earlier chapters. Poorly written specifications in a contract will lead to poorly modularized systems. Agencies with funds outside of this IDIQ process will procure based on these specifications. There are at least two methodologies in writing specifications: The turnkey and modular approaches.

OCIJ should work using the modular approach where there will be a contract for each major component. Terrestrial-WAN components are included in one contract, radio-WAN extensions in a second, and end systems (with the applications they host) are in a third.

The modular approach is better than the turnkey approach as the internet is extended to mobile platforms, it is cheaper for the agencies to procure through economies of scale, and systems have better availability (survivability).

2. Fund's Management

It is obvious that funding for any project is an important aspect for its implementation. The following are important funding issues to enhance ICT interoperability in Jordan:

Allocate an appropriate fund from governmental and the private sector for ICT interoperability research projects in Jordan. Encourage Cooperation between government

agencies, private sector, and NGO's in terms of personnel exchange, equipment, mutual fund, and aid coordination. The government should encourage this type of mutual funding which will enhance interoperability and reduce prices due the economy of scale principle.

3. JECIP Implementation Timeframe

The JECIP implementation will be based on a survey to be conducted in the country to assign locations for shelters and to pick schools, religious places, hospitals, and other public service locations to be used in case of emergency as connection nodes. These connection nodes should be chosen with specific attributes: high immunity against natural disasters, that have a backup source of power, and are easy to reach in and out.

The JECIP implementation timeframe is dependant on several factors: Available funds, policies and guideline ratification. Figure 30 depicts the implementation achievement percentage if the plan would start in Fiscal Year (FY) 2009.

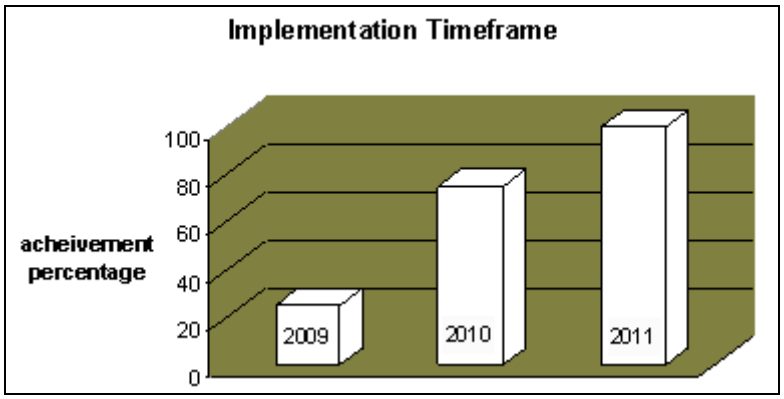

Figure 33. The JECIP Implementation Timeframe.

The implementation of the JECIP is accumulative process divided into 3 phases: preparation, implementation, and revision. In FY 2009, 25 percent of the plan will be implemented. The next two phases are based on the first step which will lead to an interoperable infrastructure in Jordan by the end of FY 2011.

F. JECIP TRAINING

Training is an important aspect of the proposed JECIP. Nationwide exercises and public awareness campaigns should be started by the authorities to prepare for the communications challenges we expect in disasters. The proposed training system for interoperable communications systems in Jordan is a triangle which includes education and training, exercise & On-the-Job-Training (OJT), and Certifications. Figure 31 depicts the Interoperability Communications Training Triangle (ICTT) in Jordan.

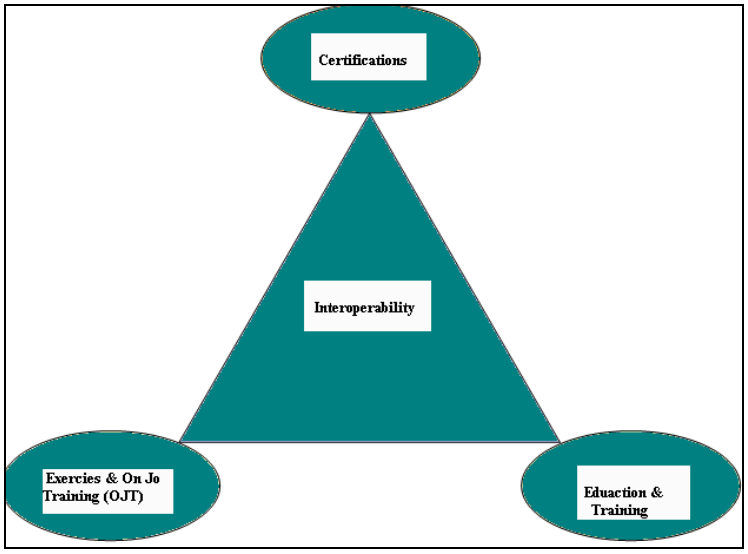

Figure 34. The Interoperability Communications Training Triangle.

1. Education and Training

Education and Training for FRC members in Jordan is a vital factor that will prepare them to work together in the field. Continuous exercise programs for agencies in Jordan should be encouraged, focusing on using the same language and terms so that they will communicate efficiently in a real disaster.

2. Exercises and On Job Training (OJT)

A knowledgeable individual that will play a key role in the acquisition of the technology should lead to interoperable systems. The current training is based on

technical training along with operational training which comes with the system procurement: training on equipment maintenance, operating the equipment and network training, and exercises in emergency communication scenarios.

Exercises similar to Strong Angel III (SAIII) should be part of the annual activities of all agencies working in the field of emergency communications. The exercises should be realistic and adhere to the available assets and limitations. It is a fact that the more that FRC members know their equipment, the more they will be able to see interoperability problems which will lead to solutions before the real emergency strikes.

3. International Cooperation

International cooperation in the communication domain of Humanitarian Assistance/Disaster Relief (HA/DR) or the Stability & Reconstruction (S&R) domain is inevitable. Mutual exercises with other countries and participation in international conferences and exercises are important to achieve ICT interoperability through exposure to other nation's experiences in this field.

4. Certifications

Currently, certification is a common methodology for measuring professionalism of FRC members. Certifications tracks for individual working in both operational and technical communications interoperability should be included as part of JECIP. The two tracks should have definitions for the three stages of training: beginner, intermediate, and professional.

G. SUMMARY

The main goal of this chapter was to propose Jordan's Emergency Communications Interoperability Plan (JECIP) and to outline guidelines to be used for improvements and enhancement of the plan with an aim of developing a more robust plan to be crafted in future.

VIII. RECOMMENDATIONS AND FUTURE WORK

Through the analysis of the different aspects of communications in emergency situations, some recommendations may be derived, such as whether Jordan should continue to invest in primarily POTS telephone infrastructure with Packet-Switching infrastructure. In the military domain, the unique nature of Jordan's Armed Forces (JAF) makes it fit for emergency response activities in the country and during peace keeping missions around the world.

The recommendations and future work introduced in this chapter may be used to enhance resilience of Information and Communications Technology (ICT) Systems in Jordan in case of emergency.

A. RECOMMENDATIONS

1. Conduct a series of seminars and workshops on JECIP and start its implementation in Fiscal year 2009.

2. Create a national JECIP steering committee that would take a holistic view of communications interoperability emergencies in Jordan and develop a compelling vision for it including definition and strategic objectives. The committee should represent both the public and private sectors.

3. Jordan should continue on a faster pace with its e-initiatives such as PC@ every home, Jordan's Broadband Learning Network, and Knowledge Stations to increase PC and Internet penetration rations.

4. Encourage cooperation between government agencies, private sector, and NGO's. This should be encouraged in terms of personnel exchanges, equipment, funds, and aid coverage.

5. Early warning systems should be deployed in identified potential likely locations of disasters.

6. Privatization of all ICT initiatives and projects is necessary to comply with WTO regulations and open competition norms which will make services better and viable infrastructure.

B. FUTURE WORK

The research in this domain is still open, and there are many things to be done. Another task would be to draft a new emergency plan for Jordan taking into account the recommendations and discussions in this thesis.

The future work on communication in emergency may be continued in the following tracks:

1. Work on an emergency communication interoperability plan for Jordanian troops participating in United Nation’s Peacekeeping missions.

2. Use the experience of different countries in the emergency communication domain to enhance Jordanian plans and procedures.

LIST OF REFERENCES

[1] Rex Buddenberg., Lecture Notes and Guidelines, available at http:/web.nps.navy.mil/~budden, last accessed April 2008.

[2] Frank Ohrtman, *WiMAX Handbook*. 105-253, McGraw-Hill Communications, Two Penn Plaza, New York, NY 10121-2298.

[3] Strong Angel III, available at http://www.strongangel3.net/, last accessed April 2007.

[4] Benton Foundation, available at www.benton.org, last accessed April 2007.

[5] International Resource group, available at www.irgltd.com, last accessed April 2007.

[6] The Tsunami Evaluation Coalition (TEC), available at http://www.tsunami-evaluation.org, last accessed April 2007.

[7] T. S. Rappaport, *Wireless Communications Principles and Practice*, pp. 105-253, Prentice Hall, Upper Saddle River, New Jersey, Second Edition.

[8] Good Practice Guide To Telecommunications Resilience, available at http://www.cpni.gov.uk/docs/re-20040501-00393.pdf, last accessed April 2008.

[9] Tracking Progress in Lower Manhattan, available at http://www.downtownny.com/files/Five%20Years%20Later.pdf, last accessed April 2008.

[10] How do Photovoltaics Work? By Gil Knier, available at http://science.nasa.gov/headlines/y2002/solarcells.htm, last accessed April 2007.

[11] Custom Power Solutions, available at http://www.mpoweruk.com/, last accessed April 2008.

[12] Telecommunications Regulatory Commission, available at http://www.trc.jo/index.php?option=com_content&task=view&id=16&Itemid=138, last accessed May 2008.

[13] FCC Enforcement Bureau's available at http://www.fcc.gov/eb/hkip/karrp.pdf, last accessed May 2008.

[14] WiFi Introduction, available at http://www.communicationspace.com/wirelessnw-wifi.html, last accessed May 2007.

[15] HFN Brown Bag and Speaker Series, available at http://www.nps.edu/cebrowski/brownbag.html, last accessed Jan 2008.

[16] David D. Lancaster, "Developing a Fly-Away-Kit (FLAK) to Support Hastily Formed Networks (HFN) for Humanitarian Assistance and Disaster Relief (HA/DR)," Master's Thesis, Naval Postgraduate School, Monterey, California, June 2005.

[17] Gary W. Thomason, " High Throughput Tactical Wireless Networking for Surveillance and Surveillance and Targeting a Coalition Environment: An Analysis of the Next Generation IEEE 802.11m Equipment and Standard" Master's Thesis, Naval Postgraduate School, Monterey, California, September 2005.

[18] The Department of Homeland Security SAFECOM communications program, available at http://www.safecomprogram.gov, last accessed Jan 2008.

[19] David Murray, & Richard Dalbello, "Satellite Industry Overview," FCC Rural Satellite Forum, January 27, 2004.

[20] Marc Kahabka, "Pocket Guide for Fundamentals and GSM Testing," available at http://www.wg.com, last accessed Jan 2008.

[21] Wireless Performance Evaluation Comparison & Applicability Report, June 1999.

[22] Susanne Lenz, "Critical Infrastructure Protection for Disaster Reduction," International Disaster Reduction Conference (IDRC) 2006 – Davos.

[23] iDEN Mobile Devices, available at http://idenphones.motorola.com/iden/, last accessed April 2008.

[24] Introduction to TETRA Technology, available at http://www.etiworld.com/wireless/tetra.pdf, last accessed April 2008.

[25] Disaster Risk Management Cycle, available at http://www.respond-int.org/respondlive/public/images/Disaster%20Risk%20Management%20Cycle.pdf /, last accessed July 2008.

[26] Noel Kirkald, "Solutions and Options for Iraq's Telecommunications Sector," Motorola, Networks, available at www.iraqdevelopmentprogram.org/idp/events/ncmc/ppt/motorola.ppt

[27] World's first WiMAX oil rig deployment, available at http://www.alandick.com/locations_americas_cellular_c2.htm, last accessed July 2008.

[28] WiMAX security, available at http://searchmobilecomputing.techtarget.com/tip/0,289483,sid40_gci1318914,00.html, last accessed July 2008.

[29] The nuts and bolts of WiMAX--Part I, available at http://www.mobilehandsetdesignline.com/howto/201302525, last accessed July 2008.

[30] Aarne Hummelholm, Postgraduate Seminar on Radio Communications, communications Laboratory, available at www.comlab.hut.fi/opetus/333/2004_2005_slides/Wireless_architectures.pdf.

[31] PicoChip's LTE and WiMAX solutions, available at www.picochip.com, last accessed July 2008.

[32] OFDM parameters in WiMAX available at http://www.WiMAX.com/commentary/WiMAX_weekly/2-3-3-ofdm-parameters-in-WiMAX-cont, last accessed July 2008.

[33] WiMAX-Architecture, available at http://www.csie.ndhu.edu.tw/~robert/mobile/WiMAX-Architecture.pdf, last accessed July 2008.

[34] Consulting, business planning and market analysis on wireless data technologies, available at http://www.senza-fili.com/, last accessed July 2008.

[35] Mobile telephony - Introduction, available at en.kioskea.net, last accessed July 2008.

[36] Future Communications Study- Action Plan 17, Final Conclusions and Recommendations report, available at http://acast.grc.nasa.gov/media/Future_Communications_Study-Action_Plan_17_DASC_2007_Fistas_Phillips_Budinger.pdf , last accessed July 2008.

[37] DIGICOM25 TETRA PMR Networks document download, available at http://www.thalesgroup.com/markets/Activities/Product-page.html, last accessed October 2008.

[38] GSMT pioneer new horizon of mobile communication presentation, available at http://www.apt.int/meetings/2005/AWF/docs/, last accessed Oct 2008.

[39] Ministry of Economic Development\ New Zealand, available at http://www.med.govt.nz , last accessed July 2008.

[40] Indefinite Delivery Indefinite Quantity (IDIQ) Contracts, available at http://www.section508.va.gov/docs/IDIQK05081.pdf, last accessed July 2008.

[41] The Global Competitiveness Report 2008-2009, available at http://gcr.weforum.org/gcr/, last accessed July 2008.

[42] The Jordanian Royal Medical Services, available at http://www.jrms.gov.jo/, last accessed November 2008.

[43] Defense Information System Agency, available at http://www.disa.mil/news/pressresources/factsheets/jitc_history.html, last accessed November 2008.

[44] Pilot Study on the Use of Telecommunications in Disaster and Emergency Situations in Sri Lanka, available at http://www.reliefweb.int/telecoms/tampere/slcs.html, last accessed November 2008.

[45] The Mobile and Internet Performance Authority, available at www.keynote.com, last accessed November 2008.

[46] Jordan's GSM coverage map, available at http://www.gsmworld.com/, last accessed November 2008.

[47] Thuraya Satellite Telecommunications, available at www.thuraya.com, last accessed December 2008.

[48] The Iridium satellite constellation, available at www.iridium.com, last accessed December 2008.

[49] 3G overview, available at www.three-g.net/3g_technology.html, last accessed December 2008.

[50] Flash-OFDM overview, available at www.cellular.co.za/flash-ofdm.htm, last accessed December 2008.

[51] The 3GPP2 Homepage, available at www.3gpp2.org/ - 3k, last accessed December 2008.

[52] Jordan's Hotspot List, available at http://www.wi-fihotspotlist.com/, last accessed December 2008.

[53] Ministry of Information and Communications Technology (MoICT), available at http://www.moict.gov.jo/MoICT/en_index.aspx, last accessed December 2008.

[54] Satellite Internet VSAT Systems available at www.vsat-systems.com, last accessed December 2008.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman, Code 37
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

4. Professor Rex Buddenberg, Code 37
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Professor David Jenn, Code EC/Jn
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

6. Lt. Col Terry Smith, Code 37
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

7. LTC Mohamad Alzaghal
   Amman
   Jordan

8. Chairman, Code SE
   Department of System Engineering
   Naval Postgraduate School
   Monterey, California

9. Professor Brian Steckler, Code IS
   Naval Postgraduate School
   Monterey, California

7. Brigadier General Mohammad Farghal
   Director of Strategic Planning
   Jordan Armed Forces (JAF)
   Amman, Jordan